

14-2985-cv

IN THE
United States Court of Appeals
FOR THE SECOND CIRCUIT

In the Matter of a Warrant to Search a Certain E-mail Account
Controlled and Maintained by Microsoft Corporation,

MICROSOFT CORPORATION,

Appellant,

— v. —

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOINT APPENDIX
VOLUME I OF II
(Pages A1 to A144)

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

Guy Petrillo
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017

E. Joshua Rosenkranz
Robert M. Loeb
Brian P. Goldman
ORRICK, HERRINGTON &
SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001

Attorneys for Appellant

(Counsel continued on inside cover)

Michael A. Levy
Justin Anderson
Assistant United States Attorneys
UNITED STATES ATTORNEY'S OFFICE
FOR THE SOUTHERN DISTRICT
OF NEW YORK
1 St. Andrew's Plaza
New York, NY 10007
(212) 637-2346

Attorneys for Appellee

TABLE OF CONTENTS

VOLUME I OF II

	Page
Docket entries	A1
Microsoft's Memorandum in Support of Motion to Vacate, Dkt. No. 6, dated Apr. 25, 2014 (redacted)	A20
Declaration of Microsoft Lead Program Manager, Dkt. No. 7, dated Apr. 25, 2014 (redacted)	A35
Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A39
Warrant, Exhibit 1 to the Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A42
Declaration of Authentication of Business Records, Exhibit 2 to the Declaration of Microsoft Program Manager, Dkt. No. 8, dated Apr. 25, 2014 (redacted)	A49
Microsoft's Reply Memorandum in Support of Motion to Vacate, Dkt. No. 10, dated Apr. 25, 2014 (redacted)	A51
Memorandum and Order, of Magistrate Judge James C. Francis IV Dkt. No. 5, dated Apr. 25, 2014	A71
Endorsed Letter Granting Stay Pending Appeal to the District Court, Dkt. No. 11, dated May 5, 2014	A98
United States Letter Not Opposing Stay Pending Appeal to the District Court, Dkt. No. 12, dated May 6, 2014	A103
Declaration of Microsoft Ireland Compliance Manager, Dkt. No. 16, dated June 6, 2014 (redacted)	A105

Declaration of Rajesh Jha, Dkt. No. 17, dated June 6, 2014 (redacted)	A107
Declaration of Michael McDowell, Dkt. No. 18, dated June 6, 2014.....	A114
Supplemental Declaration of Microsoft Lead Program Manager, Dkt. No. 19, dated June 6, 2014 (redacted)	A118
Declaration of Claire Catalano, Dkt. No. 20, dated June 6, 2014.....	A120
Email from Christopher B. Harwood to Nathan Wessler (Apr. 19, 2013), Exhibit 1 to the Declaration of Claire Catalano, dated June 6, 2014	A122
<i>How Brazil and The EU are Breaking the Internet</i> , Forbes (May 19, 2014), Exhibit 2 to the Declaration of Claire Catalano, dated June 6, 2014	A124
Letter from Sophie in't Veld to Viviane Reding (Apr. 28, 2014), Exhibit 3 to Declaration of Claire Catalano, dated June 6, 2014.....	A129
<i>Microsoft 'must release' data held on Dublin server</i> , British Broadcasting Corp. (Apr. 29, 2014), Exhibit 4 to Declaration of Claire Catalano, dated June 6, 2014.....	A131
European Commission Memorandum: Restoring Trust in EU-US data flows-Frequently Asked Questions (Nov. 27, 2013), Exhibit 5 to Declaration of Claire Catalano, dated June 6, 2014.....	A134

VOLUME II OF II

Supplemental Declaration of Claire Catalano, Dkt. No. 71, dated July 24, 2014	A145
Letter from Viviane Reding to Ms. in't Veld (June 24, 2014), Dkt. No. 71-1, dated July 24, 2014	A149
Christian Kahle, <i>US Wants to Rule over All Servers Globally</i> (July 24, 2014), Dkt. No. 71-2, dated July 24, 2014	A152

Francesco Lanza, <i>US Government to Microsoft: “Data stored online are not protected under the Fourth Amendment”</i> (July 15, 2014), Dkt. No. 71-3, dated July 24, 2014	A156
<i>US Government: Microsoft Servers Subject to US Laws, Irrespective of Country</i> , Inside Channels (July 15, 2014), Dkt. No. 71-4, dated July 24, 2014	A162
Henning Steier, <i>US Government Accessing Data on Foreign Servers</i> , Neue Zürcher Zeitung (July 15, 2014), Dkt. No. 71-5, dated July 24, 2014	A168
<i>Obama also demands access to data stored outside US</i> , Data News in Dutch (July 15, 2014), Dkt. No. 71-6, dated July 24, 2014	A174
<i>Obama Also Requires Access to Data Stored Outside of the USA</i> , Data News in French (July 15, 2014), Dkt. No. 71-7, dated July 24, 2014	A178
<i>US Government Requests Access to Data Held Abroad</i> , Der Standard (July 15, 2014), Dkt. No. 71-8, dated July 24, 2014	A182
<i>US Government: Access to Foreign Servers is Lawful</i> , Neue Osnabrücker Zeitung (July 15, 2014), Dkt. No. 71-9, dated July 24, 2014	A187
<i>US Government Requests Access to Data in EU Processing Centers</i> , Heise Online (July 15, 2014), Dkt. No.71-10, dated July 24, 2014	A192
<i>USA Also Wants Data from Foreign Servers</i> , Future Zone (July 15, 2014), Dkt. No. 71-11, dated July 24, 2014	A196
Richard Waters, <i>EU slams US over Microsoft privacy case</i> , Financial Times (June 30, 2014), Dkt. No. 71-12, dated July 24, 2014	A200

Ruadhàn Mac Cormaic, <i>High Court refers Facebook privacy case to Europe</i> , Irish Times (June 19, 2014), Dkt. No. 71-13, dated July 24, 2014	A202
<i>Maximillian Schrems v. Data Protection Commissioner</i> , 2013 No. 765JR (Irish High Court June 18, 2014), Dkt. No. 71-14, dated July 24, 2014	A205
United Kingdom’s Data Retention and Investigatory Powers Act 2014, Dkt. No. 71-15, dated July 24, 2014	A242
Declaration of Joseph V. DeMarco, Dkt. No. 72, dated July 24, 2014	A254
Supplemental Declaration of Michael McDowell, Dkt. No. 73, dated July 24, 2014	A262
Corrected Transcript of July 31, 2014 Hearing Before Chief Judge Loretta A. Preska, Dkt. No. 93, dated Sept. 9, 2014.....	A264
Endorsed Letter Granting Temporary Stay Pending Appeal, Dkt. No. 79, dated August 1, 2014	A335
Order Confirming Bench Ruling, Dkt. No. 80, dated Aug. 11, 2014	A336
Microsoft’s Notice of Appeal, Dkt. No. 81, dated Aug. 11, 2014	A337
Order Holding Microsoft in Contempt, Dkt. No. 92, dated Sept. 8, 2014.....	A339
Microsoft’s Amended Notice of Appeal, Dkt. No. 95, dated Sept. 9, 2014.....	A344

**U.S. District Court
Southern District of New York (Foley Square)
CRIMINAL DOCKET FOR CASE #: 1:13-mj-02814-UA-1**

Case title: USA v. In the matter of a Warrant to Search a
certain E-mail account controlled and maintained by Microsoft
Corporation

Date Filed: 12/04/2013

Assigned to: Judge Unassigned

Defendant (1)

**In the matter of a Warrant to Search a
certain E-mail account controlled and
maintained by Microsoft Corporation**

represented by **Brian Goldman**
Orrick, Herrington & Sutcliffe LLP (San
Francisco)
The Orrick Building
405 Howard Street
San Francisco, CA 94105
(415)-773-5676
Fax: (415)-773-4749
Email: brian.goldman@orrick.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

E. Joshua Rosenkranz
Orrick, Herrington & Sutcliffe LLP
(NYC)
51 West 52nd Street
New York, NY 10019
(212)-506-5000
Fax: (212)-506-5151
Email: jrosenkranz@orrick.com
ATTORNEY TO BE NOTICED
Designation: Retained

Guy Petrillo
Petrillo Klein & Boxer LLP
655 Third Avenue 22nd Floor
New York, NY 10017
(212) 370-0331
Fax: (212) 370-0391
Email: gpetrillo@pkblp.com
ATTORNEY TO BE NOTICED

James M. Garland
Covington & Burling

1201 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202)-662-5337
Email: jgarland@cov.com
ATTORNEY TO BE NOTICED
Designation: Retained

Nancy Lynn Kestenbaum
Covington & Burling LLP(NYC)
620 Eighth Avenue
New York, NY 10018-1405
212-841-1125
Fax: 646-441-9125
Email: nkestenbaum@cov.com
ATTORNEY TO BE NOTICED

Robert M Loeb
Orrick, Herrington & Sutcliffe, LLP
(DC)
1152 15th Street, N.W.,
Washington, DC 20005
(202)-339-8475
Fax: (202)-339-8400
Email: rloeb@orrick.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Pending Counts

None

Highest Offense Level (Opening)

None

Terminated Counts

None

Highest Offense Level (Terminated)

None

Complaints

None

Disposition**Disposition****Disposition****Amicus****Verizon Communications Inc.**represented by **Jeffrey A. Novack****A2**

Steptoe & Johnson LLP
1114 Avenue of the Americas
New York, NY 10036
212-506-3900
Fax: 212-506-3950
Email: jnovack@steptoe.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Michael Vatis
Steptoe & Johnson, LLP (NYC)
1114 Avenue of the Americas
New York, NY 10036
(212)-506-3927
Email: mvatis@steptoe.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Amicus

AT&T Corp.

represented by **Alan Charles Raul**
Sidley Austin LLP
1501 K Street
Washington, DC 20005
(202) 736-8000
Email: araul@sidley.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Charles W. Douglas
Sidley Austin LLP
10 South Dearborn Street
Chicago, IL 60603
(312) 853-7000
Email: cdouglas@sidley.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Amicus

Electronic Frontier Foundation

represented by **Hanni Fakhoury**
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415-436-9333
Fax: 415-436-9993
Email: hanni@eff.org
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Amicus**Apple Inc.**

represented by **Kenneth M. Dreifach**
Zwillgen PLLC
232 Madison Avenue
Suite 500
New York, NY 10016
646-362-5590
Fax: 202-706-5298
Email: ken@zwillgen.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kenneth Marc Dreifach
Zwillgen, PLLC
232 Madison Avenue, Suite 500
New York, NY 10016
646-362-5590
Email: ken@zwillgen.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marc J. Zwillinger
Zwillgen PLLC
1900 M St Nw, Suite 250
Washington, DC 20036
(202)-706-5202
Email: marc@zwillgen.com
ATTORNEY TO BE NOTICED

Amicus**Cisco Systems, Inc.**

represented by **Kenneth M. Dreifach**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kenneth Marc Dreifach
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marc J. Zwillinger
(See above for address)
ATTORNEY TO BE NOTICED

Amicus**Amicus Curiae Infor**

represented by **Alexander H. Southwell**
Gibson, Dunn & Crutcher, LLP
200 Park Avenue 47th, Floor
New York, NY 10166
212-351-4000
Fax: (212)-351-4035
Email: ASouthwell@gibsondunn.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Thomas G. Hungar
Gibson, Dunn & Crutcher, LLP (DC)
1050 Connecticut Avenue, N.W.
Washington, DC 20036
(202)-955-8500
Fax: (202)-467-0539
Email: thungar@gibsondunn.com
ATTORNEY TO BE NOTICED

Plaintiff**USA**

represented by **Justin A. Anderson**
United States Attorney Office, SDNY
One Saint Andrew's Plaza
New York, NY 10007
(212)-637-1035
Fax: (212) 637-2615
Email: justin.anderson@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Lorin L. Reisner
United States Attorneys Office SDNY
One Saint Andrews Plaza
New York, NY 10007
(212)637-1035
Email: reisner.lorin@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Serrin Andrew Turner
U.S. Attorney's Office, SDNY
(Chambers Street)
86 Chambers Street
New York, NY 10007
(212)-637-2701
Fax: (212)-637-2686

Email: serrin.turner@usdoj.gov

LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
12/04/2013	1	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge Michael H. Dolinger (Sealed Envelope is Document No. 14 under M9-150) (vb) (Entered: 05/29/2014)
01/30/2014	2	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge James C. Francis IV (Sealed Envelope is Document No. 31 under M9-150) (vb) (Entered: 05/29/2014)
02/24/2014	3	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge James C. Francis IV (Sealed Envelope is Document No. 42 under M9-150) (vb) (Entered: 05/29/2014)
03/14/2014	4	SEALED DOCUMENT placed in vault. So Ordered U.S. Magistrate Judge Frank Maas. (Sealed Envelope is Document No. 65 under M9-150) (vb) (Entered: 05/29/2014)
04/25/2014	5	MEMORANDUM AND ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation denying Microsoft's motion to quash the warrant in part. (Signed by Magistrate Judge James C. Francis on 4/25/14)(Filed as Document no. 93 in case M9-150) (vb) (Entered: 05/29/2014)
04/25/2014	6	REDACTED MEMORANDUM OF LAW by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support Of Microsoft's Motion to Vacate in part an SCA warrant seeking customer information located outside the U.S.. (Filed as Document no. 94 in case M9-150) (vb) (Entered: 05/30/2014)
04/25/2014	7	REDACTED DECLARATION as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support. (Filed as Document no. 95 in case M9-150)(vb) (Entered: 05/30/2014)
04/25/2014	8	REDACTED DECLARATION as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support. (Filed as Document no. 96 in case M9-150) (vb) (Entered: 05/30/2014)
04/25/2014	9	MEMORANDUM OF LAW by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Opposition. (Filed as Document no. 97 in case M9-150)(vb) (Entered: 05/30/2014)
04/25/2014	10	REDACTED REPLY MEMORANDUM OF LAW by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation in Support of Microsoft's Motion to Vacate in part an SCA warrant seeking customer information located outside the U.S.. (Filed as Document no. 98 in case M9-150) (vb) (Entered: 05/30/2014)
		A6

04/25/2014	22	INTERNET CITATION NOTE as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: Material from decision with Internet citation re: 5 Order,. (fk) (Entered: 06/09/2014)
05/05/2014	11	ENDORSED LETTER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Magistrate Judge James C. Francis IV from Guy Petrillo dated 4/30/14 re: Microsoft respectfully seeks a stay of the Order pending appeal.ENDORSEMENT: Application granted. (Signed by Magistrate Judge James C. Francis on 5/5/14)(Filed as Document no. 109 in case M9-150)(vb). (Entered: 05/30/2014)
05/06/2014	12	LETTER by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Magistrate Judge James C. Francis IV from AUSA Lorin L. Reisner dated 5/2/14 re: In response to the April 30, 2014 letter submitted by Microsoft Corp. requesting a stay pending appeal of the oder denying Microsoft's motion to vacate. The Government is prepared to consent to a stay on the condition that Microsoft seeks its appeal promptly and without any delay, so that this matter may proceed through the appropriate appeals process expeditiously Document filed by USA. (Filed as Document no. 114 in case M9-150)(vb) (Entered: 05/30/2014)
05/06/2014	13	LETTER by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Lorin L. Reisner dated May 6, 2014 re: Requesting the court to note the appearance of undersigned attorneys Lorin L. Reisner, Justin Anderson and Serrin Turner in this matter. The government also confirms it has no objection to the briefing schedule proposed by counsel for Microsoft, provided it is acceptable to the court Document filed by USA. (vb) (Entered: 05/30/2014)
05/06/2014		Attorney update in case as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Attorney Lorin L. Reisner for USA added. (vb) (Entered: 05/30/2014)
05/06/2014		Attorney update in case as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Attorney Justin A. Anderson for USA added. (vb) (Entered: 05/30/2014)
05/06/2014		Attorney update in case as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Attorney Serrin Andrew Turner for USA added. (vb) (Entered: 05/30/2014)
05/06/2014	14	ENDORSED LETTER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Guy Petrillo dated May 6, 2014 re: Notification of a proposed briefing schedule for the appeal as follows: Microsoft's Opening Memorandum of Law (30 pp.) on June 6, 2014; The Governments Opposition Memorandum of Law (30 pp.) for July 9, 2014; and Microsoft's Reply Memorandum of Law (15 pp.) for July 24, 2014. The Parties also request Oral argument at the convenience of the court.. ENDORSEMENT: The proposed briefing schedule is granted and Oral argument shall be on July 31, 2014 at 10:00 a.m. in courtroom 12A. (Signed by Judge Loretta A. Preska on 5/6/14)(vb) (Entered: 05/30/2014)
05/06/2014		Set/Reset Deadlines/Hearings as to In the matter of a Warrant to Search a certain E-

		mail account controlled and maintained by Microsoft Corporation: Microsoft's Opening Memorandum of Law due by 6/6/2014. Government's Opposition Memorandum of Law due by 7/9/2014 Microsoft's Reply Memorandum of Law due by 7/24/2014. Oral Argument set for 7/31/2014 at 10:00 AM in Courtroom 12-A, 500 Pearl Street, New York, NY 10007 before Judge Preska. (dnd) (Entered: 05/30/2014)
06/06/2014	15	Objections filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 5 Order, denying Microsoft's Motion to Vacate in part a Search Warrant seeking customer information located outside the United States. (vb) (Entered: 06/09/2014)
06/06/2014	16	DECLARATION filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
06/06/2014	17	DECLARATION of Rajesh Jha filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
06/06/2014	18	DECLARATION of Michael McDowell filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
06/06/2014	19	SUPPLEMENTAL DECLARATION filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation supplementing the Declaration of December 17, 2013. (vb) (Entered: 06/09/2014)
06/06/2014	20	DECLARATION of Claire Catalano in Support of the referenced motion, filed as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/09/2014)
06/06/2014	21	Certificate of Service of 18 Declaration, 20 Declaration in Support, 19 Declaration, 17 Declaration, 15 Reply, 16 Declaration filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on AUSA Justin Anderson on 6/6/14. (vb) (Entered: 06/09/2014)
06/10/2014	23	FILING ERROR - ELECTRONIC FILING IN NON-ECF CASE - NOTICE of Appearance as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (Novack, Jeffrey) Modified on 6/10/2014 (ka). (Entered: 06/10/2014)
06/10/2014	24	FILING ERROR - ELECTRONIC FILING IN NON-ECF CASE - MOTION to File Amicus Brief by Jeffrey A. Novack. Document filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Novack, Jeffrey) Modified on 6/10/2014 (ka). (Entered: 06/10/2014)
06/10/2014	25	FILING ERROR - ELECTRONIC FILING IN NON-ECF CASE - MEMORANDUM in Support by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re 24 MOTION to File Amicus Brief by Jeffrey A. Novack. (Novack, Jeffrey) Modified on 6/10/2014 (ka). (Entered: 06/10/2014)

06/10/2014		***NOTE TO ATTORNEY TO RE-FILE DOCUMENT - NON-ECF CASE ERROR. Note to Attorney Jeffrey Adam Novack as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: to MANUALLY RE-FILE Document Notice of Appearance, Document No. 23. This case is not ECF. (ka) (Entered: 06/10/2014)
06/10/2014		***NOTE TO ATTORNEY TO RE-FILE DOCUMENT - NON-ECF CASE ERROR. Note to Attorney Jeffrey Adam Novack as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: to MANUALLY RE-FILE Document Motion to File Amicus Brief, Document No. 24. This case is not ECF. (ka) (Entered: 06/10/2014)
06/10/2014		***NOTE TO ATTORNEY TO RE-FILE DOCUMENT - NON-ECF CASE ERROR. Note to Attorney Jeffrey Adam Novack as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: to MANUALLY RE-FILE Document Memorandum in Support, Document No. 25. This case is not ECF. (ka) (Entered: 06/10/2014)
06/10/2014	27	NOTICE of APPEARANCE as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation of Attorney Jeffrey A. Novack, Esq. of Steptoe and Johnson LLP as counsel for Verizon Communications Inc., in the above captioned matter. (vb) Modified on 6/11/2014 (vb). (Entered: 06/11/2014)
06/10/2014	28	MOTION to participate as Amicus Curiae. Document filed by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 06/11/2014)
06/10/2014	29	MEMORANDUM in Support by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re 28 MOTION to participate as Amicus Curiae and Microsoft Inc.'s Motion to Vacate Search Warrant. (vb) (Entered: 06/11/2014)
06/10/2014	30	Certificate of Service of 27 Notice (Other), 28 MOTION to participate as Amicus Curiae., 29 Memorandum in Support of Motion, by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on Lorin L. Reisner, Justin Anderson, Serrin Andrew Turner, Nancy Kestenbaum, Esq., Claire Catalano, James M. Garland, Esq., Alexander A. Berengaut, Esq., Guy Petrillo, Nelson Boxer and E. Joshua Rosenkranz on 6/10/2014. Service was made by USPS First Class Mail. (vb) (Entered: 06/11/2014)
06/11/2014		Case Designated ECF as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (do) (Entered: 06/11/2014)
06/11/2014	26	ENDORSED LETTER as to (13 Mag. 2814) In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from AUSA Serrin Turner dated June 10, 2014 re: Several prospective amici have requested the Government's consent to file amicus briefs in this matter in support of Microsoft Corporation. The Government

		does not object to the filing of amicus briefs in this litigation, so long as such briefs are kept to a reasonable length and are timely filed. Specifically, the Government respectfully requests that the Court require that any amicus brief filed in this matter not exceed 15 pages in length and that it be filed no later than June 13, 2014. ENDORSEMENT: The Government's consent is so noted. To the extent the parties are not in agreement on any details, parties requesting relief may apply to the Court by motion for leave to appear as amicus curiae. SO ORDERED. (Signed by Judge Loretta A. Preska on 6/11/2014)(bw) (Main Document 26 replaced on 6/11/2014) (bw). (Entered: 06/11/2014)
06/11/2014	31	NOTICE of Appearance by AT&T Corp. as Amicus Curiae as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (Attachments: # 1 Notice of Motion for AT&T, # 2 Memorandum of Law in Support, # 3 Declaration of Alan Charles Raul, # 4 Proposed Amicus Brief for Filing If Court Grants Motion, # 5 Corporate Disclosure Statement, # 6 Affidavit of Service)(Raul, Alan) (Entered: 06/11/2014)
06/11/2014	32	NOTICE of APPEARANCE as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation of Attorney Alan Charles Raul as counsel for AT&T Corp. (do) (Entered: 06/12/2014)
06/12/2014	33	MOTION for Leave to Appear as Amicus Curiae . Document filed by AT&T Corp. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Raul, Alan) (Entered: 06/12/2014)
06/12/2014	34	MEMORANDUM in Support by AT&T Corp. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re 33 MOTION for Leave to Appear as Amicus Curiae .. (Raul, Alan) (Entered: 06/12/2014)
06/12/2014	35	DECLARATION of Alan Charles Raul in Support by AT&T Corp. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 33 MOTION for Leave to Appear as Amicus Curiae .. (Attachments: # 1 Proposed Amicus Brief for Filing If Court Grants Motion)(Raul, Alan) (Entered: 06/12/2014)
06/12/2014	36	RULE 12.4 CORPORATE DISCLOSURE STATEMENT. identifying AT&T Inc. as Corporate Parent by AT&T Corp. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Raul, Alan) (Entered: 06/12/2014)
06/12/2014	37	Certificate of Service of 34 Memorandum in Support of Motion, 36 Rule 12.4 Corporate Disclosure Statement, 33 MOTION for Leave to Appear as Amicus Curiae ., 32 Notice (Other), 35 Declaration in Support of Motion, by AT&T Corp. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on Microsoft Corporation on 6/11/2014. Service was made by Mail. (Raul, Alan) (Entered: 06/12/2014)
06/12/2014	38	RULE 12.4 CORPORATE DISCLOSURE STATEMENT. by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Novack, Jeffrey) (Entered: 06/12/2014)

06/12/2014	39	MOTION for Michael Vatis to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9774471. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Certificates of Good Standing)(Vatis, Michael) (Entered: 06/12/2014)
06/12/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 39 MOTION for Michael Vatis to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9774471. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu) (Entered: 06/12/2014)
06/12/2014	40	Certificate of Service of 39 MOTION for Michael Vatis to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9774471. Motion and supporting papers to be reviewed by Clerk's Office staff. , 38 Rule 12.4 Corporate Disclosure Statement by Verizon Communications Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. on 6/12/2014. Service was made by Mail. (Novack, Jeffrey) (Entered: 06/12/2014)
06/13/2014	41	NOTICE of APPEARANCE as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation, Hanni Fakhoury appears for Electronic Frontier Foundation. (do) (Entered: 06/13/2014)
06/13/2014	42	MOTION for Hanni Fakhoury to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9779772. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by Electronic Frontier Foundation as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Fakhoury, Hanni) (Entered: 06/13/2014)
06/13/2014	43	Certificate of Service of 42 MOTION for Hanni Fakhoury to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9779772. Motion and supporting papers to be reviewed by Clerk's Office staff. by Electronic Frontier Foundation as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on All Parties on 06/12/2014. Service was made by Mail. (Fakhoury, Hanni) (Entered: 06/13/2014)
06/13/2014	44	MOTION for Leave to File Brief Amicus Curiae in Support of Microsoft . Document filed by Electronic Frontier Foundation as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Motion for Leave to File Brief Amicus Curiae, # 2 Exhibit A: Proposed Amicus Brief, # 3 Text of Proposed Order)(Fakhoury, Hanni) (Entered: 06/13/2014)
06/13/2014	45	Certificate of Service of 44 MOTION for Leave to File Brief Amicus Curiae in Support of Microsoft . by Electronic Frontier Foundation as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on All Parties on 06/12/2014. Service was made by Mail. (Fakhoury, Hanni) (Entered: 06/13/2014)
06/13/2014	46	RULE 12.4 CORPORATE DISCLOSURE STATEMENT. identifying None as

		Corporate Parent by Electronic Frontier Foundation as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Fakhoury, Hanni) (Entered: 06/13/2014)
06/13/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 42 MOTION for Hanni Fakhoury to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9779772. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (wb) (Entered: 06/13/2014)
06/13/2014	47	NOTICE of APPEARANCE OF Attorney Kenneth M. Dreifach for Apple Inc. and Cisco Systems, Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (do) (Entered: 06/13/2014)
06/13/2014	48	RULE 12.4 CORPORATE DISCLOSURE STATEMENT. by Apple Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Dreifach, Kenneth) (Entered: 06/13/2014)
06/13/2014	49	RULE 12.4 CORPORATE DISCLOSURE STATEMENT. by Cisco Systems, Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Dreifach, Kenneth) (Entered: 06/13/2014)
06/13/2014	50	MOTION to File Amicus Brief Document filed by Cisco Systems, Inc., Apple Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Dreifach, Kenneth) (Entered: 06/13/2014)
06/13/2014	51	MEMORANDUM in Support by Cisco Systems, Inc., Apple Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re 50 MOTION to File Amicus Brief . (Dreifach, Kenneth) (Entered: 06/13/2014)
06/13/2014	52	FILING ERROR - DEFICIENT DOCKET ENTRY - MOTION for Marc J. Zwilling to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9781280. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by Cisco Systems, Inc., Apple Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Exhibit Declaration of M. Zwilling, # 2 Text of Proposed Order)(Dreifach, Kenneth) Modified on 6/16/2014 (sdi). (Entered: 06/13/2014)
06/15/2014	53	ORDER granting 39 Motion for Michael Vatis to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 6/15/14) (vb) (Entered: 06/16/2014)
06/15/2014	54	ORDER granting 42 Motion for Hanni Fakhoury to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 6/15/14) (vb) (Entered: 06/16/2014)
06/16/2014		>>>NOTICE REGARDING DEFICIENT MOTION TO APPEAR PRO HAC VICE. Notice regarding Document No. 52 MOTION for Marc J. Zwilling to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9781280.

		Motion and supporting papers to be reviewed by Clerk's Office staff.. The filing is deficient for the following reason(s): Missing Certificate of Good Standing. Missing Certificate of Good Standing from the Supreme Court of Illinois and the District of Columbia with the Clerk of Court's signature. Missing Electronic Signature. Re-file the document as a Corrected Motion to Appear Pro Hac Vice and attach a valid Certificate of Good Standing, issued within the past 30 days. (sdi) (Entered: 06/16/2014)
06/17/2014	<u>55</u>	MOTION for Marc J. Zwillinger to Appear Pro Hac Vice (<i>Corrected</i>). Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by Cisco Systems, Inc., Apple Inc. as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # <u>1</u> Text of Proposed Order, # <u>2</u> Certificate of Good Standing, # <u>3</u> Certificate of Good Standing)(Zwillinger, Marc) (Entered: 06/17/2014)
06/17/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. <u>55</u> MOTION for Marc J. Zwillinger to Appear Pro Hac Vice (<i>Corrected</i>). Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (wb) (Entered: 06/17/2014)
07/01/2014	<u>56</u>	NOTICE of Appearance of Attorney Alexander H. Southwell for Amicus Curiae Infor, as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 07/01/2014)
07/01/2014	<u>57</u>	MOTION to File Amicus Brief by Orin Snyder. Document filed by Amicus Curiae Infor as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # <u>1</u> Text of Proposed Order, # <u>2</u> Affidavit of Service)(Southwell, Alexander) (Entered: 07/01/2014)
07/01/2014	<u>58</u>	DECLARATION of ALEXANDER H. SOUTHWELL in Support by Amicus Curiae Infor as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: <u>57</u> MOTION to File Amicus Brief by Orin Snyder.. (Attachments: # <u>1</u> Exhibit 1)(Southwell, Alexander) (Entered: 07/01/2014)
07/01/2014	<u>59</u>	MOTION for THOMAS G. HUNGAR to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9845682. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by Amicus Curiae Infor as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # <u>1</u> Certificate of Good Standing, # <u>2</u> Text of Proposed Order, # <u>3</u> Affidavit of Service)(Hungar, Thomas) (Entered: 07/01/2014)
07/02/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. <u>59</u> MOTION for THOMAS G. HUNGAR to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9845682. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (wb) (Entered: 07/02/2014)
07/09/2014	<u>60</u>	MEMORANDUM in Opposition by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re <u>24</u> MOTION to File Amicus Brief by Jeffrey A. Novack.. (Anderson, Justin) (Entered: 07/09/2014)

07/11/2014	61	ORDER granting 59 Motion for Thomas G. Hungar to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 7/10/2014) (gq) (Entered: 07/14/2014)
07/16/2014		CASHIERS OFFICE REMARK as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation on 54 Order on Motion to Appear Pro Hac Vice in the amount of \$200.00, paid on 06/13/2014, Receipt Number 465401097749. (jd) (Entered: 07/16/2014)
07/17/2014	62	ORDER granting 55 Motion for Marc J. Zwilling to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 7/17/2014) (gq) (Entered: 07/17/2014)
07/22/2014	63	NOTICE OF ATTORNEY APPEARANCE: E. Joshua Rosenkranz appearing for In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Appearance Type: Retained. (Rosenkranz, E.) (Entered: 07/22/2014)
07/22/2014	64	FILING ERROR - DEFICIENT DOCKET ENTRY - MOTION for Robert M. Loeb to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9915295. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Loeb, Robert) Modified on 7/23/2014 (wb). (Entered: 07/22/2014)
07/22/2014	65	FILING ERROR - DEFICIENT DOCKET ENTRY - MOTION for Brian P. Goldman to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9915335. Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Text of Proposed Order)(Goldman, Brian) Modified on 7/23/2014 (wb). (Entered: 07/22/2014)
07/23/2014		>>>NOTICE REGARDING DEFICIENT MOTION TO APPEAR PRO HAC VICE. Notice regarding Document No. 65 MOTION for Brian P. Goldman to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9915335. Motion and supporting papers to be reviewed by Clerk's Office staff., 64 MOTION for Robert M. Loeb to Appear Pro Hac Vice . Filing fee \$ 200.00, receipt number 0208-9915295. Motion and supporting papers to be reviewed by Clerk's Office staff.. The filing is deficient for the following reason(s): Missing Certificate of Good Standing. Re-file the document as a Corrected Motion to Appear Pro Hac Vice and attach a valid Certificate of Good Standing, issued within the past 30 days. (wb) (Entered: 07/23/2014)
07/23/2014	66	MOTION for Robert M. Loeb to Appear Pro Hac Vice . Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # 1 Certificate of Good Standing, # 2 Text of Proposed Order)(Loeb, Robert) (Entered: 07/23/2014)

07/23/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. <u>66</u> MOTION for Robert M. Loeb to Appear Pro Hac Vice . Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu) (Entered: 07/23/2014)
07/23/2014	<u>67</u>	MOTION for Brian P. Goldman to Appear Pro Hac Vice . Motion and supporting papers to be reviewed by Clerk's Office staff. Document filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Attachments: # <u>1</u> Certificate of Good Standing, # <u>2</u> Text of Proposed Order)(Loeb, Robert) (Entered: 07/23/2014)
07/23/2014		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. <u>67</u> MOTION for Brian P. Goldman to Appear Pro Hac Vice . Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu) (Entered: 07/23/2014)
07/24/2014	<u>68</u>	NOTICE OF ATTORNEY APPEARANCE: Nancy Lynn Kestenbaum appearing for In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 07/24/2014)
07/24/2014	<u>69</u>	NOTICE OF ATTORNEY APPEARANCE: Guy Petrillo appearing for In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (vb) (Entered: 07/24/2014)
07/24/2014	<u>70</u>	REPLY by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: <u>15</u> Reply, filed by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation . (Kestenbaum, Nancy) (Entered: 07/24/2014)
07/24/2014	<u>71</u>	DECLARATION of Claire Catalano in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: <u>70</u> Reply,. (Attachments: # <u>1</u> Exhibit 1, # <u>2</u> Exhibit 2, # <u>3</u> Exhibit 3, # <u>4</u> Exhibit 4, # <u>5</u> Exhibit 5, # <u>6</u> Exhibit 6, # <u>7</u> Exhibit 7, # <u>8</u> Exhibit 8, # <u>9</u> Exhibit 9, # <u>10</u> Exhibit 10, # <u>11</u> Exhibit 11, # <u>12</u> Exhibit 12, # <u>13</u> Exhibit 13, # <u>14</u> Exhibit 14, # <u>15</u> Exhibit 15)(Kestenbaum, Nancy) (Entered: 07/24/2014)
07/24/2014	<u>72</u>	DECLARATION of Joseph V. DeMarco in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: <u>70</u> Reply,. (Kestenbaum, Nancy) (Entered: 07/24/2014)
07/24/2014	<u>73</u>	DECLARATION of Michael McDowell in Support as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: <u>70</u> Reply,. (Kestenbaum, Nancy) (Entered: 07/24/2014)
07/25/2014	<u>74</u>	ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (The Oral Argument set for 7/31/14 at 10:00 a.m., is hereby adjourned to 7/31/2014 at 10:30 AM before Judge Loretta A. Preska.) (Signed by Judge Loretta A. Preska on 7/25/2014)(gq). (Entered: 07/25/2014)
07/29/2014	<u>75</u>	ORDER granting <u>67</u> Motion for Brian P. Goldman to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and

		maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 7/29/14) (vb) (Entered: 07/29/2014)
07/29/2014	76	ORDER granting 66 Motion for Robert M. Loeb to Appear Pro Hac Vice as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 7/29/14) (vb) (Entered: 07/29/2014)
07/30/2014	77	ORDER that the oral argument scheduled for July 31, 2014 at 10:30 a.m. shall be held in courtroom 26A of the U.S. Courthouse, 500 Pearl Street, New York, New York as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Signed by Judge Loretta A. Preska on 7/30/14)(vb) (Entered: 07/30/2014)
07/30/2014		Set/Reset Hearings as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: Oral Argument set for 7/31/2014 at 10:30 AM in Courtroom 26A, 500 Pearl Street, New York, NY 10007 before Judge Loretta A. Preska.. (vb) (Entered: 07/30/2014)
07/31/2014	78	LETTER by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from AUSA Serrin Turner dated 07/31/2014 re: stay pending appeal Document filed by USA. (Turner, Serrin) (Entered: 07/31/2014)
07/31/2014		MEMORANDUM TO THE DOCKET CLERK: as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. The Magistrate's decision is affirmed for the reasons set forth on the record at oral argument. So Ordered U.S.D.J. Loretta A. Preska. (vb) (Entered: 08/06/2014)
08/01/2014	79	ENDORSED LETTER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Serrin Turner dated July 31, 2014 re: Giving notice of the governments consent to a stay of the courts decision pending an appeal. ENDORSEMENT: The Stay shall extend only for such period as will permit Microsoft to file its notice of appeal, request for a stay and request for an expedited appeal. (Signed by Judge Loretta A. Preska on 8/1/14)(vb) (Entered: 08/01/2014)
08/11/2014	80	ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. This Order confirms that immediately following oral argument on July 31, 2014, for the reasons set forth on the record, the Court affirms the decision of Magistrate Judge James C. Francis IV re: 5 Order, dated April 25, 2014. (Signed by Judge Loretta A. Preska on 8/11/14) (vb) (Entered: 08/12/2014)
08/11/2014	81	NOTICE OF APPEAL by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation from 80 Order, 5 Order,. Filing fee \$ 505.00, receipt number 465401102180. (nd) (Entered: 08/12/2014)
08/12/2014		Transmission of Notice of Appeal and Certified Copy of Docket Sheet as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation to US Court of Appeals re: 81 Notice of Appeal. (nd)

		(Entered: 08/12/2014)
08/12/2014		Appeal Record Sent to USCA (Electronic File). Certified Indexed record on Appeal Electronic Files as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 81 Notice of Appeal were transmitted to the U.S. Court of Appeals. (nd) (Entered: 08/12/2014)
08/12/2014	82	LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order . Document filed by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. (Anderson, Justin) (Entered: 08/12/2014)
08/13/2014	83	Certificate of Service of 81 Notice of Appeal - Interlocutory of Notice of Appeal by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Document was served on United States on 08/11/2014. Service was made by Mail. (Goldman, Brian) (Entered: 08/13/2014)
08/18/2014	84	TRANSCRIPT of Proceedings as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: Hearing held on 7/31/2014 before Judge Loretta A. Preska. Court Reporter/Transcriber: Rebecca Forman, (212) 805-0300, Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 9/11/2014. Redacted Transcript Deadline set for 9/22/2014. Release of Transcript Restriction set for 11/20/2014. (McGuirk, Kelly) (Entered: 08/18/2014)
08/18/2014	85	NOTICE OF FILING OF OFFICIAL TRANSCRIPT as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Notice is hereby given that an official transcript of a Hearing proceeding held on 7/31/2014 has been filed by the court reporter/transcriber in the above-captioned matter. The parties have seven (7) calendar days to file with the court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript may be made remotely electronically available to the public without redaction after 90 calendar days.... (McGuirk, Kelly) (Entered: 08/18/2014)
08/19/2014	86	NOTICE OF ATTORNEY APPEARANCE: James M. Garland appearing for In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Appearance Type: Retained. (Garland, James) (Entered: 08/19/2014)
08/19/2014	87	LETTER RESPONSE to Motion by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from James M. Garland dated August 19, 2014 re: 82 LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order .. (Garland, James) (Entered: 08/19/2014)
08/20/2014	88	LETTER RESPONSE in Support of Motion by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated 8/20/14 re: 82 LETTER MOTION addressed to Judge Loretta A.

		Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order .. (Anderson, Justin) (Entered: 08/20/2014)
08/21/2014	89	NOTICE of Change of Address as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. New Address: Zwillgen PLLC, 232 Madison Avenue, Suite 500, New York, NY, United States 10016, 646-362-5590. (Dreifach, Kenneth) (Entered: 08/21/2014)
08/29/2014	90	MEMORANDUM AND ORDER granting 82 LETTER MOTION to lift the stay in execution of the Court's July 31, 2014 order as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation (1). (Signed by Judge Loretta A. Preska on 8/29/2014) (gq) (Entered: 08/29/2014)
09/04/2014	91	FILING ERROR - ELECTRONIC FILING OF NON-ECF DOCUMENT - RESPONSE by USA as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 90 Order on Letter Motion, <i>Joint Stipulation and Proposed Order</i> . (Anderson, Justin) Modified on 9/5/2014 (ka). (Entered: 09/04/2014)
09/05/2014		***NOTE TO ATTORNEY TO RE-FILE DOCUMENT - NON-ECF DOCUMENT ERROR. Note to Attorney Justin A. Anderson as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation: to E-MAIL Document to judgments@nysd.uscourts.gov., Document No. 91 Stipulation/Order. This document is not filed via ECF. (ka) (Entered: 09/05/2014)
09/08/2014	92	STIPULATION AND ORDER as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. This Court holds Microsoft Corporation in contempt for not complying in full with the warrant, and imposes no other sanctions at this time. The Government may seek sanctions in the case of materially changed circumstances in the underlying criminal investigation, or the second circuits issuance of the mandate in the appeal, if this court's order is affirmed and Microsoft continues not to comply with it. (Signed by Judge Loretta A. Preska on 9/8/14)(vb) (Entered: 09/08/2014)
09/09/2014	93	TRANSCRIPT of Proceedings as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: Hearing held on 7/31/14 CORRECTED HEARING before Judge Loretta A. Preska. Court Reporter/Transcriber: Rebecca Forman, (212) 805-0300, Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 10/3/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/11/2014. (Rodriguez, Somari) (Entered: 09/09/2014)
09/09/2014	94	NOTICE OF FILING OF OFFICIAL TRANSCRIPT as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation. Notice is hereby given that an official transcript of a Hearing proceeding held on 7/31/14 CORRECTED HEARING has been filed by the court reporter/transcriber in the above-captioned matter. The parties have seven (7) calendar days to file with the court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript may be made remotely

		electronically available to the public without redaction after 90 calendar days.... (Rodriguez, Somari) (Entered: 09/09/2014)
09/09/2014	95	AMENDED NOTICE OF APPEAL by In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation from 80 Order, 92 Stipulation and Order,,. (nd) (Entered: 09/09/2014)
09/09/2014		Transmission of Amended Notice of Appeal and Certified Copy of Docket Sheet as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation to US Court of Appeals re: 95 Amended Notice of Appeal. (nd) (Entered: 09/09/2014)
09/09/2014		First Supplemental ROA Sent to USCA (Electronic File). USCA Case No. 14-2985. Certified Supplemental Indexed record on Appeal Electronic Files as to In the matter of a Warrant to Search a certain E-mail account controlled and maintained by Microsoft Corporation re: 84 Transcript,, 93 Transcript,, 87 Response to Motion, 82 LETTER MOTION addressed to Judge Loretta A. Preska from Justin Anderson and Serrin Turner dated August 12, 2014 re: Vacatur of Stay and Enforcement of Order ., 86 Notice of Attorney Appearance - Defendant, 83 Certificate of Service, 89 Notice of Change of Address, 85 Notice of Filing Transcript,, 91 Response, 92 Stipulation and Order,, 88 Response in Support of Motion, 94 Notice of Filing Transcript,, 90 Order on Letter Motion, 95 Notice of Appeal - Interlocutory USCA Case Number 14-2985, were transmitted to the U.S. Court of Appeals. (nd) (Entered: 09/09/2014)

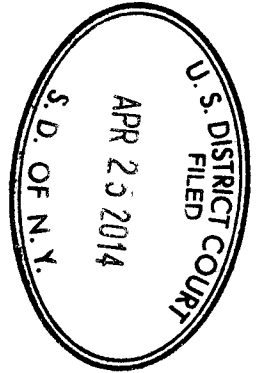
PACER Service Center

Transaction Receipt			
11/20/2014 17:26:13			
PACER			
Login:	sh0635:3867732:0	Client Code:	9843.156
Description:	Docket Report	Search Criteria:	1:13-mj-02814-UA
Billable Pages:	14	Cost:	1.40

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150



**MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN PART
AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE
THE UNITED STATES**

TABLE OF CONTENTS

	Page(s)
I. RELEVANT FACTS	1
II. ARGUMENT	5
A. Extraterritorial Warrants Are Not Authorized by Rule 41 or any Other Source of Law.	5
B. The SCA Does Not Provide an Independent Legal Basis to Obtain Electronic Communications Data Located Outside of the United States.	8
III. CONCLUSION	11

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>In re Warrant to Search a Target Computer at Premises Unknown</i> , No. H-13-234M, 2013 WL 1729765 (S.D. Tex. April 22, 2013).....	7, 8
<i>Morrison v. National Australia Bank Ltd.</i> , 130 S. Ct. 2869 (2010).....	9
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002)	8
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000).....	5
<i>United States v. Gorshkov</i> , No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001)	7
<i>United States v. Odeh</i> , 552 F.3d 157 (2d Cir. 2008).....	5
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990).....	5, 6, 7
<i>United States v. Vilar</i> , No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007).....	5, 9
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	8
<i>United States v. Williams</i> , 617 F.2d 1063 (5th Cir. 1980)	5, 6
<i>Weinberg v. United States</i> , 126 F.2d 1004 (2d Cir. 1942).....	6
<i>Zheng v. Yahoo! Inc.</i> , No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 21, 2009).....	10

STATUTES

Pub. L. No. 107-56, § 220, 115 Stat. 272 (2001).....	9
Stored Communications Act (“SCA”), 18 U.S.C. § 2703	1, 8, 9, 10

OTHER AUTHORITIES

147 Cong. Rec. H7159–03	9
Rule 41 of the Federal Rules of Criminal Procedure	5
Fed. R. Crim. P. 41, Notes	5
Department of Justice, <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> , at 85 (2009), available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf	7
Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) at 4-5, available at http://www.uscourts.gov/uscourts/RulesAndPolicies/	6

On December 4, 2013, this Court, on application of the United States, issued a search warrant directed at Microsoft Corporation (“Microsoft”) seeking customer data that, with the exception of certain non-content and address book information stored domestically, are not located in any form within the United States. Insofar as the warrant may be construed to authorize the search and seizure of data located outside the United States, Microsoft respectfully moves to vacate the warrant as unauthorized to such extent.

Courts in the United States are not authorized to issue warrants for extraterritorial searches and seizures. The result does not change because the warrant at issue here was sought under authority of the Stored Communications Act, 18 U.S.C. § 2703(a) (“SCA”). Although the SCA allows the Government to use a search warrant to obtain stored email communications from electronic communication service providers, it does not empower courts to issue warrants authorizing searches and seizures outside the United States. Nor does the SCA require electronic communication service providers to make available in the United States evidence that is not otherwise within the territorial reach of federal courts’ warrant authority.

I. RELEVANT FACTS

The warrant authorizes the search and seizure of information associated with a Microsoft web-based email account named [REDACTED]@msn.com. Declaration of [REDACTED] at ¶ 7, Ex. 1 (“[REDACTED] Decl.”). The warrant states that information associated with that account is “stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA.” *Id.* at ¶ 7, Ex. 1 at Attachment A (“Property To Be Searched”). The warrant further requires Microsoft to disclose the following information relating to the account, to the extent such information is “within [Microsoft’s] possession, custody, or control”:

1. The contents of all emails stored in the account, including copies of emails sent from the account;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the type of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
3. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
4. All records pertaining to communications between MSN or Yahoo and any person regarding the account, including contacts with support services and records of actions taken.

Id. at ¶ 7, Ex. 1 at Attachment C (“Particular Things To Be Seized”).

For many years, Microsoft has owned and operated a free, web-based email service. This service has existed at various times under different internet domain names, including, *inter alia*, Hotmail.com, MSN.com, and (since 2013) Outlook.com. See Declaration of [REDACTED] at ¶ 3 (“[REDACTED] Decl.”). Users of Microsoft web-based email accounts navigate to “Outlook.com” and log on using a username and password. *Id.* Once logged on, the user may send and receive email messages; the user may also store messages in personalized folders. *Id.*

Email message data are made up of two categories of information: (1) content information, *i.e.*, the body of an email and its subject line; and (2) non-content information about the email message, such as the sender address, recipient address, and date and time of transmission. *Id.* at ¶ 4.

Email messages sent and received by users are stored by Microsoft in Microsoft datacenters. To improve service to users, in September 2010, Microsoft began to store data for

certain web-based email accounts in a datacenter in Dublin, Ireland, which is leased and operated by Microsoft's wholly-owned Irish subsidiary, Microsoft Ireland Operations Limited. *Id.* at ¶¶ 5-6. The addition of the Dublin datacenter boosted the quality of service to users located in certain countries, for example, in Europe.¹

Microsoft stores email account data in the Dublin datacenter [REDACTED] depending on the country in which the user, when registering for email service, indicates he or she is located. [REDACTED]

Several times each day, Microsoft's software performs an automatic scan function to determine, based on the "country code" entered by the user when registering for an account, whether an account should be migrated to the Dublin datacenter. *Id.* Once an account is so migrated, all content and non-content information associated with the account in the United States is marked for deletion and subsequently deleted from Microsoft's servers in the United States.² *Id.*

The three exceptions to this framework concern certain non-content information and address book data. First, for testing and quality control purposes, Microsoft operates a "data warehouse" in the United States that stores certain non-content information relating to Microsoft web-based email accounts, including data associated with accounts hosted from the Dublin datacenter. *Id.* at ¶ 10. Second, Microsoft also operates an "address book clearing house" that contains online "address book" information relating to certain web-based email accounts,

¹ As the geographic distance between a user and a datacenter where the user's account is hosted increases, the quality of service decreases—a phenomenon known as "network latency."

See [REDACTED] Decl. at ¶ 6.

² No redundant copies of account data stored in the Dublin datacenter are stored in the United States. See [REDACTED] Decl. at ¶ 8.

including accounts hosted from Dublin. *Id.* Third, Microsoft maintains a database in the United States containing basic non-content information about web-based email accounts, such as the user's name and country provided during registration. *Id.* To the extent that the warrant calls for the search and seizure of non-content information and address book data for the account described in the warrant (e.g., categories 2-4 of Attachment C of the warrant), Microsoft has delivered the data ("Delivered Data") to the Government contemporaneously with the filing of this motion because that information is stored in the United States. [REDACTED] Decl. at ¶ 8, Ex. 2.

The content data associated with the account identified in the warrant are hosted in a datacenter in Dublin, Ireland. A member of Microsoft's Global Criminal Compliance ("GCC") team,³ located in the United States, made this determination by logging into a database management program [REDACTED] See *id.* at ¶ 7. The GCC team member entered identifying information concerning the account [REDACTED] and determined the location of the user data. *Id.* [REDACTED]

[REDACTED]

[REDACTED] *Id.*

³ The GCC team handles all responses to search warrants for stored electronic communications data.

II. ARGUMENT

A. **Extraterritorial Warrants Are Not Authorized by Rule 41 or any Other Source of Law.**

Neither Rule 41 of the Federal Rules of Criminal Procedure, nor any other rule or statute, authorizes the issuance of warrants to be executed outside the territory of the United States. *See United States v. Vilar*, No. 05-CR-621, 2007 WL 1075041, at *52 (S.D.N.Y. Apr. 4, 2007) (“[A]s other courts have observed, there is no statutory basis for a magistrate judge in the Southern District of New York to issue a search warrant in a non-terrorism case targeting property in the Eastern District of New York, let alone to issue such a warrant to be executed in London, England.”); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) (holding that “there is presently no statutory basis for the issuance of a warrant to conduct searches abroad”). Indeed, the Supreme Court expressly rejected a proposed amendment to Rule 41 that would have permitted the issuance of warrants authorizing searches for property outside of the United States. *See* Fed. R. Crim. P. 41, Notes of Advisory Committee on Rules — 1990 Amendment.

In the absence of any rule of procedure or statutory authority, courts have not recognized any inherent authority to issue warrants seeking property outside of the United States. In *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008), for instance, the Second Circuit observed that “seven justices of the Supreme Court [in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)] endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches,” *id.* at 169, and held that “it is by no means clear that U.S. judicial officers *could be* authorized to issue warrants for overseas searches,” *id.* at 171 (emphasis added).⁴ In *United*

⁴ *See Verdugo-Urquidez*, 494 U.S. at 279 (Stevens, J., concurring) (“I do not believe the Warrant Clause has any application to searches of noncitizens’ homes in foreign jurisdictions (continued...)”).

States v. Williams, 617 F.2d 1063 (5th Cir. 1980), the Fifth Circuit, sitting *en banc*, similarly observed that “there is substantial doubt that the federal district courts have the authority to issue [extraterritorial] warrant[s].” *Id.* at 1072; *see also Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1942) (observing that “[w]ith very few exceptions, United States district judges possess no extraterritorial jurisdiction,” and construing statute authorizing issuance of search warrants as limited by the court’s territorial jurisdiction).

The Government itself has recognized it cannot conduct warranted searches outside the United States. In a recent request to amend Rule 41, the Government described its proposed amendment as consistent with the presumption against extraterritoriality and explained that the amendment “does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.” Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) at 4-5, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/cr-suggestions-2013/13-CR-B-Suggestion_Raman.pdf. In fact, the Government recognized that even under its proposed amendment, “should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect.” *Id.*

This warrant calls for the disclosure of content data that can only be obtained through an extraterritorial search and seizure. [REDACTED]

because American magistrates have no power to authorize such searches.”); *id.* at 278 (Kennedy, J., concurring) (remarking upon the “[t]he absence of local judges or magistrates available to issue [extraterritorial] warrants”); *id.* at 297 (Blackmun, J., dissenting) (“[A]n American magistrate’s lack of power to authorize a search abroad renders the Warrant Clause inapplicable to the search of a noncitizen’s residence outside this country.”).

[REDACTED]

[REDACTED] In other words, the search and seizure would take place in Ireland, not the United States. See, e.g., *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (holding that federal agents' "extraterritorial access to computers in Russia" constituted "a search or seizure of . . . property outside the territory of the United States" (citing *Verdugo-Urquidez*, 494 U.S. 259));⁵ *In re Warrant to Search a Target Computer at Premises Unknown*, No. H-13-234M, 2013 WL 1729765 (S.D. Tex. April 22, 2013) (rejecting Government's application for a search warrant under Rule 41 where the Government "admits that the current location of the Target Computer is unknown," and emphasizing that the location of the data — not the location of the searching agents — determines the location of the search for purposes of Rule 41); accord U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at 85 (2009), available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> ("When agents learn before a search that some or all of the data is stored remotely outside of the United States, matters become more complicated. The United States may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned," even though "the search may seem domestic to a U.S. law enforcement officer executing the search in the United States pursuant to a valid warrant . . .").

⁵ In *Gorshkov*, the Government did not initially obtain a warrant; rather, federal agents in Seattle surreptitiously obtained the defendant's computer passwords and then used them to access remotely one of the defendant's computers located in Russia. 2001 WL 1024026, at *1. The court ultimately rejected the defendant's motion to suppress on the grounds that the Fourth Amendment did not apply to the agents' extraterritorial search of a non-resident alien's property. *Id.* at *3. Because the Government in this case sought and obtained a warrant, the ultimate question addressed by the court in *Gorshkov* is not presented here.

The warrant was issued under the authority of the SCA presumably on the assumption that all data sought are located in the United States. (As noted above, Microsoft already has produced to the Government the Delivered Data located in the United States.) The content data sought by the warrant, however, are located in Dublin, Ireland. The warrant is not valid to authorize the search and seizure of this evidence.

B. The SCA Does Not Provide an Independent Legal Basis to Obtain Electronic Communications Data Located Outside of the United States.

Nothing in the SCA or its legislative history suggests that it may be used to reach the contents of electronic communications in foreign countries. The scope of the Government's authority to seek content data under the SCA is defined by the valid scope of the warrant at issue. The statute provides that the Government in these circumstances must obtain "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure" (or the procedures provided under applicable state laws). 18 U.S.C. § 2703(a); *see also United States v. Warshak*, 631 F.3d 266, 283 (6th Cir. 2010) ("The government may obtain the contents of e-mails that are in electronic storage with an electronic communication service for 180 days or less only pursuant to a warrant." (internal quotation marks omitted)). The warrant here cannot authorize the search and seizure of property located outside the United States — whether or not the Court issued it under the authority of the SCA.

Moreover, it bears emphasis that Microsoft has received a *warrant* under the SCA, and not a subpoena. The two forms of process are distinct. *See United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) ("While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants." (citing 18 U.S.C. § 2703(b)(1)(A))). Unlike subpoenas, search warrants may not be used to compel production of evidence located outside the United States if it is

merely within the provider's "possession, custody, or control." Permitting search warrants to be used like subpoenas in this way would effectively vest the Government with power to accomplish indirectly (through the assistance of an electronic communication service provider) what it could not do directly — namely, conduct a warranted extraterritorial search.

In addition, the plain meaning of the SCA does not authorize extraterritorial warrants. As the Supreme Court recently reaffirmed in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869 (2010), "unless there is the affirmative intention of the Congress clearly expressed to give a statute extraterritorial effect, we must presume it is primarily concerned with domestic conditions." *Id.* at 2877 (internal quotation marks and citation omitted). "When a statute gives no clear indication of an extraterritorial application, it has none." *Id.* at 2878.

Nothing in the SCA's text or legislative history suggests that the law is meant to authorize warrants for extraterritorial searches. Rather, when Congress amended the SCA in 2001 to provide that search warrants could be issued by a magistrate judge with jurisdiction over the offense under investigation, even for electronic data located outside of the judge's district, the very title of the amendment was "*Nationwide Service of Search Warrants for Electronic Evidence.*" Pub. L. No. 107-56, § 220, 115 Stat. 272 (2001) (emphasis added); *see also Vilar*, 2007 WL 1075041 at *52 n.33 (observing that "nothing in the language of [the 2001 SCA] amendment remotely suggests that the power [of a magistrate judge to authorize a search outside of his or her district] extended to extraterritorial searches"). The legislative history confirms that this amendment to the SCA "[p]ermits a single court having jurisdiction over the offense to issue a search warrant for e-mail that would be valid . . . anywhere in the United States." 147 Cong. Rec. H7159-03 at H7197-98 (emphasis added).

The absence of authority in the SCA for extraterritorial warrants is confirmed by the ruling of at least one federal district court, which explicitly rejected the argument that the Electronic Communications Privacy Act (“ECPA”), which includes the SCA, applies extraterritorially. In *Zheng v. Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 21, 2009), the court held that ECPA does not apply outside the United States, and further noted that Congress had not made clear, through either ECPA’s text or legislative history, its intent that the law apply outside the United States. *See id.* *2–4 (internal quotation marks and citation omitted).⁶

Neither does the SCA compel a private electronic communication service provider, such as Microsoft, to cause data outside the United States to be transferred into the United States in response to a search warrant. As the text of the statute makes clear, the recipient of a warrant under the SCA must act upon receipt of a *valid* warrant. A warrant is not valid insofar as it is used for the search and seizure of material outside the United States; thus, under the SCA, no action is required by Microsoft to cause electronic data outside the United States to be transported to the United States.

In short, the SCA does not authorize extraterritorial warrants. Accordingly, insofar as the warrant here may be construed to authorize the search and seizure of data located outside the United States, Microsoft respectfully moves to vacate the warrant to such extent.

⁶ Notably, the court in *Zheng* held that ECPA did not apply to interceptions that took place abroad, even if the emails, prior to their disclosure “travelled electronically through a network located in the United States.” *Id.* at *4.

III. CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Court vacate that part of the warrant calling for the search and seizure of customer information located outside the United States.

Dated: December 18, 2013

Respectfully submitted,

MICROSOFT CORPORATION



Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkblp.com
nboxer@pkblp.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

**Applications for admission pro hac vice
pending*

Counsel for Microsoft Corporation

C # 95

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Action Nos. 13-MAG-2814, M9-150

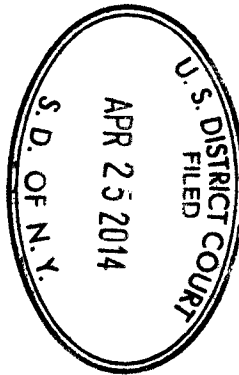
Declaration Of [REDACTED]

I, [REDACTED] declare as follows:

1. I am a Lead Program Manager for Microsoft Corporation. I have worked for Microsoft since 2002. I have a B.S. from Stanford University and have worked in Hotmail/Outlook.com as an infrastructure Program Manager/Lead Program Manager during my tenure at Microsoft.

2. In my current position, I am responsible for managing the storage "backend" for Outlook.com, which is the current Internet domain name for Microsoft's web-based customer email service. This means that I manage the software and hardware that stores Outlook.com users' emails in Microsoft datacenters so that they can be accessed remotely by users from a variety of mobile and desktop computing devices. I have personal knowledge of the facts stated in this declaration.

3. Microsoft has owned and operated free, web-based email since at least 1997, and this service has operated at various times under different domain names, including Hotmail.com, MSN.com, and Outlook.com. Outlook.com was created in 2013. Users with Outlook.com accounts log on to the service by navigating to the "Outlook.com" web address and by providing their usernames and passwords. Users can also access Outlook.com through their mobile



devices. Once they have logged in, users are able to send and receive email messages and store messages in personalized folders.

4. Email messages contain two basic categories of information. First, messages contain content information: the body of an email and its subject line. Second, messages contain non-content information about the email message, such as its sender, the address of its recipient, and the date and time of transmission.

5. Messages sent and received by users of Microsoft's web-based email services are stored in Microsoft datacenters. Microsoft, through its wholly-owned Irish subsidiary, Microsoft Ireland Operations Limited, leases and operates a datacenter in Dublin, Ireland. Starting in September 2010, Microsoft began storing data for certain web-based email accounts in the Dublin datacenter. [REDACTED]

[REDACTED] Microsoft stores email account data in the Dublin datacenter depending on information provided by the user during the account registration process. Specifically, when a user first activates a new account, he or she is asked a series of questions, including "Where are you from?" In response to this question, a user must choose a country from a drop-down menu, and each country is assigned a unique country code. Accounts associated with certain country codes are hosted from the Dublin datacenter [REDACTED]

6. Microsoft decides where to store email account data in part to reduce "network latency." Network latency is the principle of network architecture that the greater the geographic distance between a user and the datacenter where the user's data is stored, the slower the service.

The advantage of storing email account data in Dublin is that it allows Microsoft to enhance network efficiency for its users.

7. [REDACTED]

[REDACTED] Several times each day, Microsoft's backend software runs an automatic scan to determine whether newly-created accounts should be migrated to the Dublin datacenter based on their country code. Once an account is migrated to the Dublin datacenter, all content and non-content information associated with the account in the United States is marked for deletion and is subsequently deleted from Microsoft's U.S.-based servers.

8. For each web-based email account, several copies of the email content and non-content information are created for purposes of redundancy, and the redundant copies are updated on a continuous basis. For accounts stored in Dublin, none of the redundant copies of data are stored in the United States.

9. With the three exceptions discussed below, web-based email user data stored in Dublin is not stored in the United States. Thus, with these three exceptions, if Microsoft were to receive a legal demand from the government for user data stored in Dublin, the only way to access that data would be from the Dublin datacenter.

10. The three exceptions referred to above are: (1) for testing and quality control purposes, Microsoft operates a "data warehouse" in the United States that contains certain non-content information about web-based email accounts, including accounts stored in Dublin; (2) for certain web-based email accounts, including accounts hosted from Dublin, users' online "address book" information is stored in Microsoft's "address book clearing house" ("ABCH"), another centralized database stored on servers in the United States; and (3) Microsoft maintains

in the United States a database of basic non-content information about web-based email user accounts, such as the name and country provided during registration.

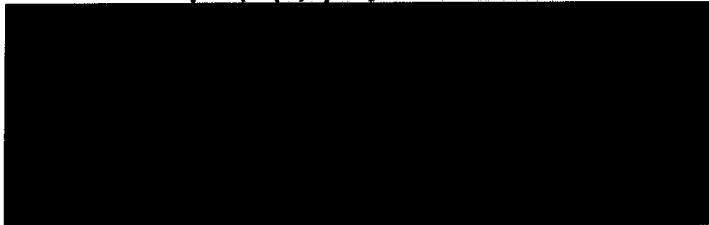
11. Subject to these three exceptions, all account information associated with Microsoft web-based email accounts hosted in Dublin is stored exclusively in Dublin and can be accessed only from the Dublin datacenter.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated:

12/17/13

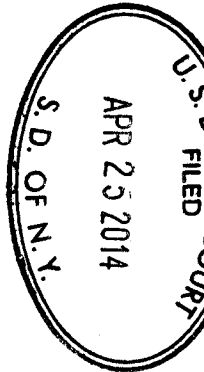


DOC # 96

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Action Nos. 13-MAG-2814, M9-150

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation



Declaration Of [REDACTED]

I, [REDACTED], declare as follows:

1. I am a Program Manager for Microsoft Corporation. I have worked for Microsoft since 2009. I attended Carnegie Mellon from 2005-2009 and received a BS in computer science. I have worked on Microsoft's web-based email services since 2009.

2. In my current position, I am responsible for the tools used to respond to requests by law enforcement agencies for information stored by Microsoft's web-based email service, which currently is called Outlook.com. I have personal knowledge of the facts stated in this declaration.

3. When Microsoft receives a search warrant for stored electronic information, the Global Criminal Compliance ("GCC") team is responsible for handling the response. The GCC team works from offices in the United States (in California and Washington).

4. The GCC team uses a database management program [REDACTED]


[REDACTED] tool to collect the data sought by search warrants. The [REDACTED] tool [REDACTED]

[REDACTED] is accessed via

a web user interface.

5. When collecting email account data sought by a search warrant, a GCC team member first determines the location of the Microsoft server on which the data is stored. To do this, the GCC team member logs into [REDACTED] and enters certain identifying information about the user account for which data is sought. The [REDACTED] tool then locates the account and determines where data for the account is stored.

6. Once a GCC team member has located the data, the team member may then [REDACTED] collect the requested information from the server on which the user's account is stored.



7. I have reviewed the warrant issued to Microsoft on December 4, 2013, by the United States District Court for the Southern District of New York (the "Warrant"). A true and accurate copy of the Warrant is attached to this declaration as Exhibit 1. I have entered the account information from the Warrant [REDACTED] determined the location of the user data, and ascertained that the data for the targeted account is stored on Microsoft's servers in Microsoft's datacenter in Dublin, Ireland.

8. I also attach to this declaration as Exhibit 2 a true and accurate copy of a custodian of records form prepared by GCC, certifying that any information associated with the

targeted user account that may be stored in the United States has been produced to the Government.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: 12/17/13

Signed:

A large black rectangular redaction box covering the signature area.

Exhibit 1

AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New York**13 MAG 2814**In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)

Case No.

The PREMISES known and described as the email account)
[REDACTED]@MSN.COM, which is controlled by Microsoft Corporation)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(Identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [REDACTED]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.

☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court.

JCMJ Initials

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).

☐ Until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013

4:32 pm

James C. Francis IV
Judge's signatureCity and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY

Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with

██████████@msn.com, which is stored at premises owned,
maintained, controlled, or operated by Microsoft Corporation, a
company headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT C

Particular Things To Be Seized

I. Information To Be Disclosed By MSN [REDACTED]:

To the extent that the information described in Attachment A for MSN, [REDACTED], is within the possession, custody, or control of MSN [REDACTED], then MSN [REDACTED] is required to disclose the following information to the Government for each account or identifier listed in Attachment A [REDACTED] (the "TARGET ACCOUNT") for the period of inception of the account to the present:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files,

and means and sources of payment (including any credit or bank account number);

- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All records pertaining to communications between MSN [REDACTED] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information To Be Seized By The Government

A variety of techniques may be employed to search the seized e-mails for evidence of the specified crimes, including but not limited to keyword searches for various names and terms including the TARGET SUBJECTS, and other search names and terms; and email-by-email review.

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 21, United States Code, Sections 846, 959, 960, and 963, Title 46, United States Code, Section 70503, and Title 18, United States Code, Section 1956, including, for each account or identifier listed on Attachment A [REDACTED], information pertaining to the following matters:

- a. Any communications:

1. Pertaining to narcotics, narcotics trafficking, importation of narcotics into the United States, money laundering, or the movement or distribution of narcotics proceeds;

2. [REDACTED]
[REDACTED];

3. Pertaining to the use of ports or other places of entry to receive or ship narcotics or narcotics proceeds;

4. Related to the physical location of the TARGET SUBJECTS and their co-conspirators;


5. Constituting evidence of who uses the TARGET ACCOUNT, and where they live and work, and where they are using the TARGET ACCOUNT; and

6. Constituting information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

Exhibit 2

RE: GCC-562972-J9D5H8

DECLARATION OF AUTHENTICATION OF BUSINESS RECORDS
(Pursuant to Federal Rules of Evidence 803(6) and 902(11))

I, , am the Custodian of Records, or am otherwise qualified to authenticate the records of Microsoft Corporation. Microsoft Corporation has provided the attached records pursuant to a Search Warrant.

I hereby certify that the attached records are business records of the regularly conducted activity, and that I am a custodian or am otherwise qualified as to the authentication of these records. I also certify that these records are:

1. made at or near the time of the occurrence of the matter set forth in the records by a person with knowledge of those matters or for information transmitted by a person with knowledge of those matters; and are true copies of the original records described in the Search Warrant and are stored on Microsoft servers inside the United States.
2. kept in the course of regularly conducted activity; and were made by the regularly conducted activity as a regular practice.
3. made by the regularly conducted activity as a regular practice.

The address and phone number where I can be reached at are:

Microsoft Corporation
1065 LaAvenida, Mountain View, CA 94043
425-722-1299

I declare under penalty of perjury under the laws of the State of California, that the foregoing is true and correct.

Signed: 

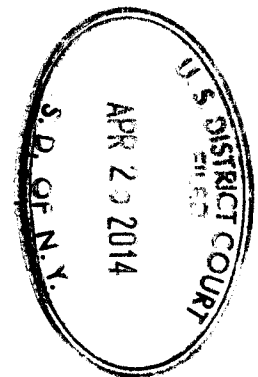
Dated this December 17, 2013

DOC # 98

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150



REPLY MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN
PART AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED
OUTSIDE THE UNITED STATES

TABLE OF CONTENTS

	Page(s)
I. U.S. Courts Lack The Authority to Issue Extraterritorial Warrants.	2
II. The Instrument at Issue Is an Extraterritorial Warrant, Not a Subpoena or Any Other Form of Compulsory Process The Government Tries to Read Into the SCA.....	3
III. Search Warrants Safeguard Constitutionally Protected Privacy Interests and Are Fundamentally Different From Subpoenas.	7
IV. The Government’s Policy Arguments Fail to Address Important Considerations That Undercut its Position	11
V. Conclusion	13

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Am. Tobacco Co. v. Patterson</i> , 456 U.S. 63 (1982).....	4
<i>Almeida-Sanchez v. United States</i> , 413 U.S. 266 (1973).....	13
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	8
<i>In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Address</i> , Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917 (D. Kan. Sept. 21, 2012).....	5
<i>Conn. Nat'l Bank v. Germain</i> , 503 U.S. 249 (1992).....	4, 5
<i>In re Grand Jury Proceedings (Bank of Nova Scotia)</i> , 740 F.2d 817 (11th Cir. 1984)	7
<i>Hubbard v. MySpace, Inc.</i> , 788 F. Supp. 2d 319 (S.D.N.Y. 2011).....	6
<i>In re Marc Rich & Co., A.G.</i> , 707 F.2d 663 (2d Cir. 1983).....	8
<i>Morrison v. Nat'l Australia Bank Ltd.</i> , 130 S. Ct. 2869 (2010).....	7, 8
<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000)	9, 10
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002)	5
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000).....	2
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	8
<i>United States v. Davis</i> , 767 F.2d 1025 (2d Cir. 1985).....	12

<i>United States v. Gorshkov</i> , No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001)	3
<i>United States v. Odeh</i> , 552 F.3d 157 (2d Cir. 2008).....	2
<i>United States v. Vilar</i> , No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007).....	2
<i>In re Warrant to Search a Target Computer at Premises Unknown</i> , No. H-13-234M, 2013 WL 1729765 (S.D. Tex. April 22, 2013).....	3, 4
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	9, 10
<i>United States v. Zovluck</i> , 274 F. Supp. 385 (S.D.N.Y. 1967)	8
 Statutes	
18 U.S.C. § 2703(a)	5, 6, 10
18 U.S.C. § 2703(b)(1)(A)	10
18 U.S.C. § 2703(b)(1)(B)	4, 10
18 U.S.C. § 2703(d)	6
18 U.S.C. § 2703(g)	6
18 U.S.C. § 2705(a)(1)(B)	10
18 U.S.C. § 2705(a)(2).....	10
18 U.S.C. § 2709.....	6
18 U.S.C. § 2711.....	4
50 U.S.C. § 1805.....	6

Other Authorities

U.S. Const. amend. IV	5
Mutual Legal Assistance Treaty Between the United States and Ireland, T.I.A.S, 13137	11
FED. R. CRIM. P. 17(c)(2)	8
FED. R. CRIM. P. 41	3, 5, 6, 7
FED. R. CRIM. P. 41(b)(1)	3
RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987)	12
Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Rcena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 20 13), available at http://www.uscourts.gov/uscourts/RulesAndPolicies/	7
Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union (April 19, 2013), <i>available at</i> : https://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf	10
United States Attorney Manual ("USAM") 9:279, available at: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm	12

The Government has served Microsoft with a warrant that seeks, among other things, the contents of a customer's email. Upon inspection, Microsoft determined that the email content data is stored in Ireland and is not located in any form within the United States. There is no dispute that this Court lacks the authority to issue a warrant empowering the Government to execute a search and seizure in Ireland. And yet, the Government insists it should be permitted to compel Microsoft's assistance in doing *indirectly* precisely what it lacks the authority to do *directly* — *i.e.*, conduct a warranted search outside the United States.

The Government seeks to defend its position by arguing that this case does not involve an extraterritorial search and seizure at all. In the Government's view, because the warrant was directed at Microsoft Corporation in the United States, Microsoft is obligated — as it arguably would be if it received a grand jury subpoena — to produce responsive data located anywhere in the world, so long as that data is within Microsoft's possession, custody, or control. In other words, the Government argues that when Congress, in 1986, used the word "warrant" in the Stored Communications Act ("SCA"), it did not mean warrant as that word has been used and understood in criminal law for centuries. Rather, according to the Government, Congress meant to create an entirely new form of warrant (what the Government calls an "SCA Warrant") that functions like a subpoena and therefore can be used to compel an electronic communication service provider to produce data stored outside the United States.

The Government cannot cite a single case in which *any* court has *ever* interpreted the term "warrant" in the SCA to mean "subpoena." This is not surprising. The Government's interpretation ignores both the plain meaning of the SCA and the well-established principle that federal statutes are presumed to lack extraterritorial effect. The Government's interpretation also contravenes long-standing precedent regarding the distinctions between warrants and subpoenas,

ignores the constitutional interests that underlie those distinctions, and upsets the delicate comity analysis that is necessary — and that the Government admits is required — when the United States seeks to compel a private party to produce evidence located abroad.

I. U.S. Courts Lack The Authority to Issue Extraterritorial Warrants.

Microsoft has established, and the Government has not contested, that courts in the United States lack the power to issue warrants authorizing extraterritorial searches and seizures. *See* Memorandum in Support of Microsoft’s Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside the United States (“Br.”) at 5 (citing *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008) (concluding that U.S. courts are not empowered to issue warrants for foreign searches); *United States v. Vilar*, No. 05-CR-621, 2007 WL 1075041, at *52 (S.D.N.Y. Apr. 4, 2007) (finding no statutory basis for court to issue search warrant to be executed abroad); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) (same)).

Given the complete absence of authority for extraterritorial warrants, the Government attacks straw man arguments. For instance, rather than addressing the import of the decisions Microsoft cites, the Government recasts them to stand for the wholly irrelevant point that “the Warrant Clause does not limit the Government’s ability to gather evidence overseas.” Government’s Memorandum of Law in Opposition to Microsoft’s Motion to Vacate Email Account Warrant (“Op.”) at 13. Microsoft is not asking the Court to decide whether the Fourth Amendment prohibits the Government from gathering evidence overseas *without a warrant*. The question is whether *the warrant issued in this case* compels Microsoft to assist in an extraterritorial search. The answer must be no. Courts lack the authority to issue extraterritorial warrants, and the SCA only requires Microsoft to comply with a *valid* warrant.

The Government similarly misstates Microsoft's position as being that Rule 41 *forbids* such warrants when issued under the SCA. Op. at 13 ("Microsoft is equally mistaken to suggest that the substantive limitations on conventional search warrants directed to physical premises, as set forth in Rule 41 ... have any impact on SCA warrants"). What Microsoft argues, however, is that "extraterritorial warrants are not *authorized* by Rule 41 or any other source of law." Br. at 5 (emphasis added and capitalization omitted). The Government fails entirely to address this absence of authority — which is confirmed by, *inter alia*, the Supreme Court's express rejection in 1990 of an amendment to Rule 41 that would have authorized extraterritorial search warrants. See Br. at 5.¹

II. The Instrument at Issue Is an Extraterritorial Warrant, Not a Subpoena or Any Other Form of Compulsory Process The Government Tries to Read Into the SCA.

Having little to say about extraterritorial warrants, the Government next argues that the warrant served on Microsoft is *not* extraterritorial because it is "not directed at a physical location" but rather is served on Microsoft Corporation in the United States. Op. at 16. The courts have been clear, however, that a search of electronic data occurs where the data is stored, not at the point(s) from which it may be remotely accessed. See Br. at 7 (citing *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001); *In re Warrant to Search a Target Computer at Premises Unknown*, No. H-13-234M, 2013 WL

¹ The Government's reliance on the 2001 amendment to the SCA is misplaced. See Op. at 13-14. That amendment authorized the issuance of search warrants by a magistrate judge with jurisdiction over the offense under investigation for electronic data located in a district other than the district of the magistrate judge. The amendment was necessary because such out-of-district warrants would ordinarily be contrary to Rule 41. See FED. R. CRIM. P. 41(b)(1) (authorizing a magistrate judge to "issue a warrant to search for and seize a person or property *located within the district*" (emphasis added)). As we explained in our opening brief, nothing in this amendment empowered magistrate judges to issue out-of-district warrants authorizing the search and seizure of data located outside the United States. See Br. at 9.

1729765 (S.D. Tex. April 22, 2013)). Here, some of the relevant user data is located in Ireland. The warrant therefore purports to authorize a search that would take place in Ireland. *See id.* at 6-8. That should end the analysis. But rather than addressing this point, or the case law Microsoft cites, the Government attempts to rewrite the SCA to avoid the limitations of a warrant altogether.

The Government first suggests that the term “warrant” in the SCA does not actually mean “warrant” but instead means “subpoena.” This ignores the most basic rule of statutory construction. “[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (citations and internal quotation marks omitted); *see also Am. Tobacco Co. v. Patterson*, 456 U.S. 63, 68 (1982) (“As in all cases involving statutory construction, our starting point must be the language employed by Congress, and we assume that the legislative purpose is expressed by the ordinary meaning of the words used.” (alteration, citations, and internal quotation marks omitted)).

There is no reason to think Congress actually meant “subpoena” when it used the word “warrant.” The definitional section of the SCA, 18 U.S.C. § 2711, does not assign a meaning to the word “warrant,” much less one that differs from its well-established meaning. And when Congress actually wanted to use the word “subpoena” in the SCA, it had no difficulty doing so. *See, e.g.*, 18 U.S.C. § 2703(b)(1)(B) (authorizing the government to compel the disclosure of information “if the governmental entity ... uses an administrative *subpoena* authorized by Federal or State statute or a Federal or State grand jury or trial *subpoena*.” (emphasis added)).

Faced with the fact that Congress chose the word “warrant” and not “subpoena,” the Government suggests next that when Congress enacted the SCA, it created an entirely novel

form of compulsory process — which the Government terms an “SCA Warrant” — that operates *like* a subpoena and can compel a provider to produce data stored anywhere in the world. The SCA, however, says nothing about “SCA Warrants.” Nor does the statute suggest that Congress meant to vest federal courts with the power to issue “worldwide warrants.” To the contrary, the SCA authorizes the government to compel providers to disclose information “only pursuant to a *warrant* issued using the procedures described in the Federal Rules of Criminal Procedure” 18 U.S.C. § 2703(a) (emphasis added). Congress used the term “warrant,” and it must be assumed that it “says in a statute what it means.” *Conn. Nat’l Bank*, 503 U.S. at 254. As the Eighth Circuit observed in *United States v. Bach*, “[w]hile warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants.” 310 F.3d 1063, 1066 n.1 (8th Cir. 2002).²

In fact, the SCA does not in any way *create* authority for courts to issue warrants. Section 2703(a) merely authorizes the government to compel providers to produce information if served with a warrant — in other words, to provide assistance to the Government in executing the underlying warrant. The statute thus incorporates by reference an existing form of compulsory process derived from other established sources of law, including the Fourth Amendment and Fed. R. Crim. P. 41. See *In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-8191-DJW Target Email Address*, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, *5 (D. Kan. Sept. 21, 2012) (“A warrant seeking stored electronic communications such as emails or faxes therefore should be subject to

² The Government criticizes the court’s decision in *Bach* for not “elaborat[ing] on its reasoning or the implications of its observations,” and asserts that the quoted language was an “academic point” made in a footnote. Op. at 17-18 & n.11. But the Government fails to identify any flaw in the *Bach* court’s common-sense conclusion that Congress intended “warrants” issued under the SCA to be treated like warrants and not like subpoenas. See *id.*

the same basic requirements of any search warrant”). Where Congress has sought to create new forms of compulsory process, both in the SCA and in other statutes, it has done so clearly. *See, e.g.*, 18 U.S.C. § 2703(d) (authorizing disclosure orders based on “specific and articulable facts showing that there are reasonable grounds to believe that the [information is] relevant and material to an ongoing criminal investigation”); 18 U.S.C. § 2709 (authorizing “National Security Letters” to compel production of certain non-content information); 50 U.S.C. § 1805 (authorizing surveillance orders under the Foreign Intelligence Surveillance Act based on probable cause). Here, however, Congress decided not to create a new form of process but opted instead to rely on the pre-existing warrant authority.

Nor does the fact that the SCA abrogates specific aspects of Rule 41 support the Government’s interpretation. The Government notes that (i) the SCA requires that warrants comply only with the “procedures described in” Rule 41 (*i.e.*, not its substantive provisions), and (ii) the statute eliminates the traditional requirement of an officer’s presence when a warrant is executed. *See Op.* at 14 (citing 18 U.S.C. § 2703(a), (g); *Hubbard v. MySpace, Inc.*, 788 F. Supp. 2d 319, 325 n.18 (S.D.N.Y. 2011)). This does not imply that Congress intended to create a new type of “worldwide warrant.” If anything, it shows the opposite. Specifically, Congress chose to draft the SCA to include narrowly tailored changes to pre-existing warrant procedures, but at the same time declined to alter the well-established principle that courts lack authority to issue extraterritorial warrants.

In arguing to the contrary, the Government runs squarely into the presumption against extraterritoriality. The Government claims that “neither the text nor the structure of the SCA *limits* the scope of compelled disclosure . . . to records maintained within the United States.” *Op.* at 6 (capitalization omitted and emphasis added). This approach to statutory interpretation is

upside down. The Supreme Court has explained unequivocally that “[w]hen a statute gives no clear indication of an extraterritorial application, it has none.” *Morrison v. Nat’l Australia Bank Ltd.*, 130 S. Ct. 2869, 2878 (2010). The SCA contains no indication, let alone a *clear* indication, that Congress intended warrants issued under the statute to authorize the search and seizure of data located outside the United States — a proposition with which the Government has expressly agreed in proposing amendments to Rule 41. See Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, to Judge Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) (the “Raman Letter”) (“In light of the presumption against international extraterritorial application ... this [proposed] amendment [to Rule 41] does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.”).³

III. Search Warrants Safeguard Constitutionally Protected Privacy Interests and Are Fundamentally Different From Subpoenas.

The Government strains to interpret “warrant” in the SCA to mean “subpoena” so as to take advantage of a line of cases often referred to as the *Bank of Nova Scotia* (or “BNS”) doctrine. These cases hold that a party subject to U.S. jurisdiction can be compelled by grand jury subpoena to produce evidence stored outside the United States so long as the evidence is within the party’s “possession, custody, or control.” See Op. at 9 (citing, *inter alia*, *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984)).⁴ While the

³ The Government soft-pedals the Raman Letter by excerpting several inapposite passages, see Op. at 15-16, but it tellingly has nothing to say about the letter’s key acknowledgement (quoted above) that the SCA does not authorize courts to issue warrants for extraterritorial searches and seizures.

⁴ Microsoft does not concede that the BNS doctrine is good law after the Supreme Court’s reinvigoration of the presumption against extraterritoriality in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869, 2878 (2010). The Court need not address this issue because even if (continued...)

Government cites several cases for the basic *BNS* principle, it fails to identify *any* in which a court has applied *BNS* in the context of a search warrant. We are aware of none.

The Government's inability to support its argument with actual precedent is not a coincidence. Warrants and grand jury subpoenas are fundamentally different types of legal process. The grand jury is vested with "wide latitude to inquire into violations of criminal law," *United States v. Calandra*, 414 U.S. 338, 343 (1974), and when it issues a subpoena, the recipient is compelled as a matter of "public duty" to collect and produce the responsive evidence. *In re Marc Rich & Co., A.G.*, 707 F.2d 663, 670 (2d Cir. 1983). And notably, the recipient of a grand jury subpoena may move the court *ex ante* to modify or quash the subpoena. See FED. R. CRIM. P. 17(c)(2).

A warrant, in contrast, is a constitutionally limited, *ex parte* authorization from a court that permits the Government to trespass upon private property. Unlike a subpoena-recipient, the target of a warranted search is neither able to contest the search *ex ante* nor "required to aid in the discovery, production, or authentication of incriminating evidence." *Andresen v. Maryland*, 427 U.S. 463, 473-74 (1976). Moreover, "[t]he authority to search [granted by a warrant] is limited to the place described in the warrant and does not include additional or different places." *United States v. Zovluck*, 274 F. Supp. 385, 390 (S.D.N.Y. 1967). Warrants thus authorize a narrow yet fundamentally more intrusive exercise of government power than the self-directed process called for by a subpoena. As noted by the Fourth Circuit, "the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the

the *BNS* doctrine survives *Morrison*, it does not apply to warrants for the reasons discussed herein.

issuance of a subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded.” *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000).

Despite the historical and fundamental differences between the two forms of process, the Government takes the extraordinary position that Microsoft has engaged in a “muddled reading” of the SCA by simply giving effect to the plain meaning of the word “warrant.” The Government argues that this reading would be contrary to the statute’s “upside-down pyramid” structure insofar as law enforcement could conceivably compel the disclosure of more information with a subpoena than with a warrant. *See* Op. at 7-8 (“It cannot be that Congress intended that a subpoena can properly require a service provider to produce emails regardless of where they are stored, but a 2703(d) Order or SCA Warrant — issued pursuant to higher standards and court approval — imposes more limited obligations on a U.S. service provider.”). But given that the subpoena power is exercised on notice to the customer or subscriber whose data is sought by the subpoena, and may sweep more broadly than the warrant authority, the claimed “absurdity” identified by the Government is illusory. The Government’s argument fails for two reasons.

First, the SCA “upside-down pyramid” that the Government portrays is, in practice, no pyramid at all — at least not since 2010, when the Sixth Circuit held that the Fourth Amendment requires the Government to obtain a warrant to search for and seize email content. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). We understand that the Government’s practice since *Warshak* has been to obtain a warrant when seeking access to email contents in

criminal cases.⁵ Given that the Government appears only to use the warrant section of the SCA when seeking the contents of stored electronic communications, its structural argument rings hollow.

Second, and more fundamentally, the Government's argument ignores the SCA's use of different notice provisions for the different forms of process. If the Government serves a warrant under the SCA, it is not required to notify the customer, *see* 18 U.S.C. § 2703(a), (b)(1)(A) — a practice that is consistent with established precedent applicable to physical searches and seizures. *See In re Subpoena Duces Tecum*, 228 F.3d at 348 (“A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things. To preserve advantages of speed and surprise, the order is issued *without prior notice* and is executed, often by force, with an unannounced and unanticipated physical intrusion” (emphasis added)).

In contrast, the subpoena power under the SCA is generally exercised *on notice* to the customer or subscriber whose data is sought, and may therefore have a wider reach than the warrant authority. *See* 18 U.S.C. § 2703(b)(1)(B).⁶ The SCA's notice requirement for subpoenas permits the customer to vindicate his or her privacy (or other) interests by moving to quash the subpoena. *See In re Subpoena Duces Tecum*, 228 F.3d at 348 (“A subpoena, on the

⁵ *See* Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union (April 19, 2013) (confirming that the United States Attorney's Office for the Southern District of New York has not, since *Warshak*, “authorized a request to a court for access to the contents of a person's private electronic communications for law enforcement purposes without a warrant or on a standard less than probable cause”), *available at*: <https://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf>.

⁶ The SCA allows the Government to delay notice to the target of a subpoena for ninety days “upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result[.]” 18 U.S.C. § 2705(a)(1)(B), with the term “adverse result” defined with particularity in the statute. *See id.* § 2705(a)(2).

other hand [*i.e.*, unlike a warrant], commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, *and its justification derives from*, that process.” (emphasis added)).

In short, subpoenas have a wider reach than warrants, but the statute provides an opportunity to challenge them *ex ante*. Warrants, while more intrusive than subpoenas, are at the same time more limited; they are constrained both by the Fourth Amendment’s requirements of probable cause and particularity, and by the inherent inability of federal courts to authorize searches and seizures outside the United States. This trade-off, embedded in the structure of the SCA, makes eminent sense. The Government’s muddling of the distinction between the two forms of process makes no sense.

IV. The Government’s Policy Arguments Fail to Address Important Considerations That Undercut its Position.

The Government argues that Microsoft’s motion should be denied as a matter of policy because it would “severely undercut criminal investigations.” *Op.* at 19. It bases its argument on the mistaken notion that “Microsoft appears to believe that the mere fact that records are stored abroad renders them beyond the scope of compulsory process.” *Id.* Microsoft did not say this. Indeed, the Government could compel it to disclose email content stored in Dublin by proceeding under the Ireland-United States Mutual Legal Assistance Treaty (“MLAT”), which entered into force on August 11, 2009. *See* Mutual Legal Assistance Treaty Between the United States and Ireland, T.I.A.S. 13137. The Government shrugs off this alternative by complaining that “Mutual Legal Assistance Treaties and letters rogatory are slow and cumbersome processes.” *Op.* at 21. But even if this is true (and the Government offers no evidence it is), inconvenience cannot justify a blatant disregard of the SCA’s plain language.

Considerations of international comity further undercut the Government's policy arguments. The Second Circuit has explicitly recognized that the law of foreign jurisdictions may forbid compliance with subpoenas that seek data stored within their borders, and has held that international comity may justify limitations on the Government's subpoena power. *See United States v. Davis*, 767 F.2d 1025, 1033-34 (2d Cir. 1985) (adopting a multi-factor analysis set out in the Restatement of Foreign Relations Law "in evaluating the propriety of a subpoena directing the production of information or documents located abroad when such production would violate the law of the state in which the documents are located"); *see also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987).

The Government itself recognizes that *Bank of Nova Scotia* subpoenas can threaten international relations. According to the United States Attorneys' Manual, "foreign governments strongly object to [*BNS*] subpoenas, contending that they constitute an improper exercise of United States jurisdiction." United States Attorney Manual ("USAM") 9:279, available at: http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm.⁷

⁷ In deciding whether to approve a *BNS* subpoena, the USAM requires federal prosecutors to weigh the following considerations:

- 1) The availability of alternative methods for obtaining the records in a timely manner, such as use of mutual assistance treaties, tax treaties or letters rogatory;
- 2) The indispensability of the records to the success of the investigation or prosecution; and
- 3) The need to protect against the destruction of records located abroad and to protect the United States' ability to prosecute for contempt or obstruction of justice for such destruction.

Id.

Where a subpoena calls for data stored outside the United States, a motion to quash provides an orderly mechanism for courts to conduct a *Davis* multi-factor comity analysis before requiring the production of data in violation of foreign law. Warrant procedures do not provide this mechanism. In fact, the Government and courts may not always know whether a warrant calls for the production of data stored outside the United States, which would make it impossible for either the Government or the court issuing the warrant to consider the comity principles articulated in *Davis* and the USAM. These troubling consequences are avoided if warrants directed at electronic communications service providers for communications data covered by the SCA are interpreted under traditional principles of territoriality, as the plain language of the statute requires.

In short, the Government's policy concerns do not change the text of the SCA, nor should they create authority for extraterritorial warrants where none exists. Microsoft freely concedes that the plain meaning of the SCA may constrain the Government's exercise of investigative powers. That is nothing new in our constitutional system. As the Supreme Court observed in *Almeida-Sanchez v. United States*, "[t]he needs of law enforcement stand in constant tension with the Constitution's protections of the individual against certain exercises of official power. It is precisely the predictability of these pressures that counsels a resolute loyalty to constitutional safeguards." 413 U.S. 266, 273 (1973).


V. Conclusion


For the foregoing reasons and those set forth in its opening brief, Microsoft respectfully requests that the Court vacate that part of the warrant calling for the search and seizure of customer information located outside the United States.

Dated: March 14, 2014

Respectfully submitted,

MICROSOFT CORPORATION


Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017
Tel: 212.370.0330
gpetrillo@pkblp.com
nboxer@pkblp.com


Nancy Kestenbaum SDNY Bar # NK9768
Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
nkestenbaum@cov.com
ccatalano@cov.com

James M. Garland*
Alexander A. Berengaut*
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401
Tel: 202.662.6000
Fax: 202.662.6291
jgarland@cov.com
aberengaut@cov.com

**Admitted pro hac vice*

Counsel for Microsoft Corporation

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Search of The PREMISES
known and described as the email account
[REDACTED]@MSN.COM, which is
controlled by Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

CERTIFICATE OF SERVICE

I, Claire Catalano, hereby certify that on the 14th Day of March, 2014, I caused a true and correct copy of the REPLY MEMORANDUM IN SUPPORT OF MICROSOFT'S MOTION TO VACATE IN PART AN SCA WARRANT SEEKING CUSTOMER INFORMATION LOCATED OUTSIDE THE UNITED STATES to be served via hand delivery upon the United States Attorney for the Southern District of New York at the following address:

ATTN: Andrea Surratt
United States Attorney for the Southern District of New York
One St. Andrews Plaza
New York City, NY 10007



Claire Catalano SDNY Bar # CC7432
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
Tel: 212-841-1000
Fax: 212-841-1010
ccatalano@cov.com

DOC # 93

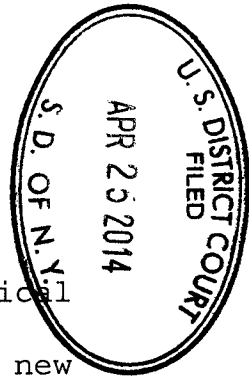
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - :
IN THE MATTER OF A WARRANT TO :
SEARCH A CERTAIN E-MAIL ACCOUNT :
CONTROLLED AND MAINTAINED BY :
MICROSOFT CORPORATION :
- - - - - :

M9-150
13 Mag. 2814

MEMORANDUM
AND ORDER

JAMES C. FRANCIS IV
UNITED STATES MAGISTRATE JUDGE



"The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign." David R. Johnson & David Post, Law and Borders -- The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1375 (1996). In this case I must consider the circumstances under which law enforcement agents in the United States may obtain digital information from abroad. Microsoft Corporation ("Microsoft") moves to quash a search warrant to the extent that it directs Microsoft to produce the contents of one of its customer's e-mails where that information is stored on a server located in Dublin, Ireland. Microsoft contends that courts in the United States are not authorized to issue warrants for extraterritorial search and seizure, and that this is such a warrant. For the reasons that follow, Microsoft's motion is denied.

Background

Microsoft has long owned and operated a web-based e-mail service that has existed at various times under different internet domain names, including Hotmail.com, MSN.com, and Outlook.com. (Declaration of A.B. dated Dec. 17, 2013 ("A.B. Decl."), ¶ 3).¹ Users of a Microsoft e-mail account can, with a user name and a password, send and receive email messages as well as store messages in personalized folders. (A.B. Decl., ¶ 3). E-mail message data include both content information (the message and subject line) and non-content information (such as the sender address, the recipient address, and the date and time of transmission). (A.B. Decl., ¶ 4).

Microsoft stores e-mail messages sent and received by its users in its datacenters. Those datacenters exist at various locations both in the United States and abroad, and where a particular user's information is stored depends in part on a phenomenon known as "network latency"; because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter. (A.B. Decl., ¶ 6). Accordingly, based on

¹ Pursuant to an application by Microsoft, certain information that is commercially sensitive, including the identity of persons who submitted declarations, has been redacted from public filings.

the "country code" that the customer enters at registration, Microsoft may migrate the account to the datacenter in Dublin. (A.B. Decl., ¶ 7). When this is done, all content and most non-content information associated with the account is deleted from servers in the United States. (A.B. Decl., ¶ 7).

The non-content information that remains in the United States when an account is migrated abroad falls into three categories. First, certain non-content information is retained in a data warehouse in the United States for testing and quality control purposes. (A.B. Decl., ¶ 10). Second, Microsoft retains "address book" information relating to certain web-based e-mail accounts in an "address book clearing house." (A.B. Decl., ¶ 10). Finally, certain basic non-content information about all accounts, such as the user's name and country, is maintained in a database in the United States. (A.B. Decl., ¶ 10).

On December 4, 2013, in response to an application by the United States, I issued the search warrant that is the subject of the instant motion. That warrant authorizes the search and seizure of information associated with a specified web-based e-mail account that is "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA." (Search and Seizure Warrant ("Warrant")), attached as Exh. 1 to Declaration of C.D. dated Dec.

17, 2013 ("C.D. Decl."), Attachment A). The information to be disclosed by Microsoft pursuant to the warrant consists of:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All records pertaining to communications between MSN . . . and any person regarding the account, including contacts with support services and records of actions taken.

(Warrant, Attachment C, ¶ I(a)-(d)).

It is the responsibility of Microsoft's Global Criminal Compliance ("GCC") team to respond to a search warrant seeking stored electronic information. (C.D. Decl., ¶ 3). Working from offices in California and Washington, the GCC team uses a database program or "tool" to collect the data. (C.D. Decl., ¶¶ 3, 4). Initially, a GCC team member uses the tool to determine where the data for the target account is stored and then collects the

information remotely from the server where the data is located, whether in the United States or elsewhere. (C.D. Decl., ¶¶ 5, 6).

In this case, Microsoft complied with the search warrant to the extent of producing the non-content information stored on servers in the United States. However, after it determined that the target account was hosted in Dublin and the content information stored there, it filed the instant motion seeking to quash the warrant to the extent that it directs the production of information stored abroad.

Statutory Framework

The obligation of an Internet Service Provider ("ISP") like Microsoft to disclose to the Government customer information or records is governed by the Stored Communications Act (the "SCA"), passed as part of the Electronic Communications Privacy Act of 1986 (the "ECPA") and codified at 18 U.S.C. §§ 2701-2712. That statute authorizes the Government to seek information by way of subpoena, court order, or warrant. The instrument law enforcement agents utilize dictates both the showing that must be made to obtain it and the type of records that must be disclosed in response.

First, the Government may proceed upon an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. § 2703(b)(1)(B)(i). In response, the service provider must produce (1) basic customer

information, such as the customer's name, address, Internet Protocol connection records, and means of payment for the account, 18 U.S.C. § 2703(c)(2); unopened e-mails that are more than 180 days old, 18 U.S.C. § 2703(a); and any opened e-mails, regardless of age, 18 U.S.C. §§ 2703(b)(1)(B)(i).² The usual standards for

² The distinction between opened and unopened e-mail does not appear in the statute. Rather, it is the result of interpretation of the term "electronic storage," which affects whether the content of an electronic communication is subject to rules for a provider of electronic communications service ("ECS"), 18 U.S.C. § 2703(a), or those for a provider of remote computing service ("RCS"), 18 U.S.C. § 2703(b). The SCA regulates the circumstances under which "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication [] that is in electronic storage in an electronic communications system" 18 U.S.C. § 2703(a). "Electronic storage" is in turn defined as "(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17). While most courts have held that an e-mail is no longer in electronic storage once it has been opened by the recipient, see, e.g., Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771-73 (C.D. Ill. 2009); see also Owen S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1216 (2004) (hereinafter A User's Guide) ("The traditional understanding has been that a copy of an opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules"), the Ninth Circuit has instead focused on whether "the underlying message has expired in the normal course," Theofel v. Farley-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004); see also id. at 1077 ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage."). Resolution of this debate is unnecessary for purposes of the issue before me.

Likewise, it is not necessary to determine whether Microsoft

issuance of compulsory process apply, and the SCA does not impose any additional requirements of probable cause or reasonable suspicion. However, the Government may obtain by subpoena the content of e-mail only if prior notice is given to the customer. 18 U.S.C. § 2703(b)(1)(B)(i).

If the Government secures a court order pursuant to 18 U.S.C. § 2703(d), it is entitled to all of the information subject to production under a subpoena and also "record[s] or other information pertaining to a subscriber [] or customer," such as

was providing ECS or RCS in relation to the communications in question. The statute defines ECS as "any service which provides users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), while RCS provides "to the public [] computer storage or processing services by means of an electronic communications system, 18 U.S.C. § 2711(2). Since service providers now generally perform both functions, the distinction, which originated in the context of earlier technology, is difficult to apply. See Crispin, 717 F. Supp. 2d at 986 n.42; In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) (hereinafter In re United States) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself."); Kerr, A User's Guide at 1215 ("The distinction of providers of ECS and RCS is made somewhat confusing by the fact that most network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in some contexts, and as neither in some contexts as well.").

historical logs showing the e-mail addresses with which the customer had communicated. 18 U.S.C. § 2703(c)(1). In order to obtain such an order, the Government must provide the court with "specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d).

Finally, if the Government obtains a warrant under section 2703(a) (an "SCA Warrant"), it can compel a service provider to disclose everything that would be produced in response to a section 2703(d) order or a subpoena as well as unopened e-mails stored by the provider for less than 180 days. In order to obtain an SCA Warrant, the Government must "us[e] the procedures described in the Federal Rules of Criminal Procedure" and demonstrate probable cause. 18 U.S.C. § 2703(a); see Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants).

Discussion

Microsoft's argument is simple, perhaps deceptively so. It notes that, consistent with the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the Government sought information here by means of a warrant. Federal courts are without authority to issue warrants for the search and seizure of property outside the

territorial limits of the United States. Therefore, Microsoft concludes, to the extent that the warrant here requires acquisition of information from Dublin, it is unauthorized and must be quashed.

That analysis, while not inconsistent with the statutory language, is undermined by the structure of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it.

A. Statutory Language

In construing federal law, the "starting point in discerning congressional intent is the existing statutory language." Lamie v. United States Trustee, 540 U.S. 526, 534 (2004) (citing Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999)). "And where the statutory language provides a clear answer, [the analysis] ends there as well." Hughes Aircraft Co., 525 U.S. at 438. However, a court must search beneath the surface of text that is ambiguous, that is, language that is "capable of being understood in two or more possible senses or ways." Chickasaw Nation v. United States, 534 U.S. 84, 90 (1985) (internal quotation marks omitted).

Here, the relevant section of the SCA provides in pertinent part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only

pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.

18 U.S.C. § 2703(a). This language is ambiguous in at least one critical respect. The words "using the procedures described in the Federal Rules of Criminal Procedure" could be construed to mean, as Microsoft argues, that all aspects of Rule 41 are incorporated by reference in section 2703(a), including limitations on the territorial reach of a warrant issued under that rule. But, equally plausibly, the statutory language could be read to mean that while procedural aspects of the application process are to be drawn from Rule 41 (for example, the presentation of the application based on sworn testimony to a magistrate judge), more substantive rules are derived from other sources. See In re United States, 665 F. Supp. 2d at 1219 (finding ambiguity in that "'[i]ssued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41"); In re Search of Yahoo, Inc., No. 07-3194, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (finding that "the phrase 'using the procedures described in' the Federal Rules remains ambiguous"). In light of this ambiguity, it is appropriate to look for guidance in the "statutory structure, relevant legislative history, [and] congressional purposes."

Florida Light & Power Co. v. Lorion, 470 U.S. 729, 737 (1985); see Board of Education v. Harris, 444 U.S. 130, 140 (1979); Hall v. EarthLink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).

B. Structure of the SCA

The SCA was enacted at least in part in response to a recognition that the Fourth Amendment protections that apply in the physical world, and especially to one's home, might not apply to information communicated through the internet.

Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime. When we use a computer network such as the Internet, however, a user does not have a physical "home," nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.

This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications -- or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all.

See Kerr, A User's Guide at 1209-10 (footnotes omitted).

Accordingly, the SCA created "a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between

government investigators and service providers in possession of users' private information." Id. at 1212. Because there were no constitutional limits on an ISP's disclosure of its customer's data, and because the Government could likely obtain such data with a subpoena that did not require a showing of probable cause, Congress placed limitations on the service providers' ability to disclose information and, at the same time, defined the means that the Government could use to obtain it. See id. at 1209-13.

In particular, the SCA authorizes the Government to procure a warrant requiring a provider of electronic communication service to disclose e-mail content in the provider's electronic storage. Although section 2703(a) uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question.

This unique structure supports the Government's view that the SCA does not implicate principles of extraterritoriality. It has

long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information. See Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983) ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location." (citations omitted)); Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147-48 (S.D.N.Y. 2011) ("If the party subpoenaed has the practical ability to obtain the documents, the actual physical location of the documents -- even if overseas -- is immaterial."); In re NTL, Inc. Securities Litigation, 244 F.R.D. 179, 195 (S.D.N.Y. 2007); United Sates v. Chase Manhattan Bank, N.A., 584 F. Supp. 1080, 1085 (S.D.N.Y. 1984). To be sure, the "warrant" requirement of section 2703(a) cabins the power of the government by requiring a showing of probable cause not required for a subpoena, but it does not alter the basic principle that an entity lawfully obligated to produce information must do so regardless of the location of that information.

This approach is also consistent with the view that, in the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer." Orin S. Kerr,

Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005). In this case, no such exposure takes place until the information is reviewed in the United States, and consequently no extraterritorial search has occurred.

This analysis is not undermined by the Eighth Circuit's decision in United States v. Bach, 310 F.3d 1063 (8th Cir. 2002). There, in a footnote the court noted that "[w]e analyze this case under the search warrant standard, not under the subpoena standard. While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants." Id. at 1066 n.1. Given the context in which it was issued, this sweeping statement is of little assistance to Microsoft. The issue in Bach was whether the fact that a warrant for electronic information was executed by employees of the ISP outside the supervision of law enforcement personnel rendered the search unreasonable in violation of the Fourth Amendment. Id. at 1065. The court utilized the stricter warrant standard for evaluating the reasonableness of the execution of a search, as opposed to the standard for executing a subpoena; this says nothing about the territorial reach of an SCA Warrant.

C. Legislative History

Although scant, the legislative history also provides support for the Government's position. When the SCA was enacted as part of

the ECPA, the Senate report, although it did not address the specific issue of extraterritoriality, reflected an understanding that information was being maintained remotely by third-party entities:

The Committee also recognizes that computers are used extensively today for the processing and storage of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. . . . [B]ecause it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

S. Rep. No. 99-541, at 3 (1986).

While the House report did address the territorial reach of the law, it did so ambiguously. Because the ECPA amended the law with respect to wiretaps, the report notes:

By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example it . . . regulates only those "interceptions" conducted within the territorial United States. Similarly, the controls in Section 201 of the Act [which became the SCA] regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

H.R. Rep. 99-647, at 32-33 (1986) (citations omitted). While this language would seem to suggest that information stored abroad would

be beyond the purview of the SCA, it remains ambiguous for two reasons. First, in support of its observation that the ECPA does not regulate activities outside the United States, the Committee cited Stowe v. DeVoy, 588 F.2d 336 (2d Cir. 1978). In that case, the Second Circuit held that telephone calls intercepted in Canada by Canadian authorities were admissible in a criminal proceeding even if the interception would have violated Title III of the Omnibus Crime Control Act of 1968 if it had occurred in the United States or been performed by United States officials. Id. at 340-41. This suggests that Congress was addressing not the reach of government authority, but rather the scope of the individual rights created by the ECPA. Second, in referring to "access" to stored electronic communications, the Committee did not make clear whether it meant access to the location where the electronic data was stored or access to the location of the ISP in possession of the data.

Additional evidence of congressional intent with respect to this latter issue can be gleaned from the legislative history of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "Patriot Act"). Section 108 of the Patriot Act provided for nationwide service of search warrants for electronic evidence. The House Committee described the rationale for this as follows:

Title 18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section does not affect the requirement for a search warrant, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the "warrant" be obtained "within the district" where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain the warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned.

Section 108 amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located.

H.R. Rep. 107-236(I), at 58 (2001). This language is significant, because it equates "where the property is located" with the location of the ISP, not the location of any server. See In re Search of Yahoo, Inc., 2007 WL 1539971, at *4 ("Commentators have suggested that one reason for the amendments effected by Section 220 of the Patriot Act was to alleviate the burden placed on federal district courts in the Eastern District of Virginia and the Northern District of California where major internet service providers [] AOL and Yahoo, respectively, are located.") (citing, inter alia, Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375, 1454 (2004)).

Congress thus appears to have anticipated that an ISP located in the United States would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control, regardless of where that information was stored.³

D. Practical Considerations

If the territorial restrictions on conventional warrants applied to warrants issued under section 2703(a), the burden on the Government would be substantial, and law enforcement efforts would be seriously impeded. If this were merely a policy argument, it would be appropriately addressed to Congress. But it also provides context for understanding congressional intent at the outset, for it is difficult to believe that, in light of the practical consequences that would follow, Congress intended to limit the reach of SCA Warrants to data stored in the United States.

First, a service provider is under no obligation to verify the information provided by a customer at the time an e-mail account is opened. Thus, a party intending to engage in criminal activity could evade an SCA Warrant by the simple expedient of giving false

³ Suppose, on the contrary, that Microsoft were correct that the territorial limitations on a conventional warrant apply to an SCA warrant. Prior to the amendment effected by the Patriot Act, a service provider could have objected to a warrant issued by a judge in the district where the provider was headquartered on the basis that the information sought was stored on a server in a different district, and the court would have upheld the objection and quashed the subpoena. Yet, I have located no such decision.

residence information, thereby causing the ISP to assign his account to a server outside the United States.

Second, if an SCA Warrant were treated like a conventional search warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty ("MLAT"). As one commentator has observed, "This process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other." Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Penn. L. Rev. 373, 409 (2014). Moreover, nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance. For example, the MLAT between the United States and Canada provides that "[t]he Requested State may deny assistance to the extent that . . . execution of the request is contrary to its public interest as determined by its Central Authority." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Can., March 18, 1985, 24 I.L.M. 1092 ("U.S.-Can. MLAT"), Art. V(1). Similarly, the MLAT between the United States and the United Kingdom allows the Requested State to deny assistance if it deems that the request would be "contrary to important public policy" or involves "an offense of a political character." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, S. Treaty Doc. No. 104-2 ("U.S.-U.K. MLAT"), Art. 3(1)(a) &

(c)(i). Indeed, an exchange of diplomatic notes construes the term "important public policy" to include "a Requested Party's policy of opposing the exercise of jurisdiction which is in its view extraterritorial and objectionable." Letters dated January 6, 1994 between Warren M. Christopher, Secretary of State of the United States, and Robin W. Renwick, Ambassador of the United Kingdom of Great Britain and Northern Ireland (attached to U.S.-U.K. MLAT). Finally, in the case of a search and seizure, the MLAT in both of these examples provides that any search must be executed in accordance with the laws of the Requested Party. U.S.-Can. MLAT, Art. XVI(1); U.S.-U.K. MLAT, Art. 14(1), (2). This raises the possibility that foreign law enforcement authorities would be required to oversee or even to conduct the acquisition of information from a server abroad.

Finally, as burdensome and uncertain as the MLAT process is, it is entirely unavailable where no treaty is in place. Although there are more than 60 MLATs currently in force, Amy E. Pope, Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches, 65 Fla. L. Rev. 1917, 1931 (2013), not all countries have entered into such agreements with the United States. Moreover, Google has reportedly explored the possibility of establishing true "offshore" servers: server farms located at sea beyond the territorial jurisdiction of any nation.

Steven R. Swanson, Google Sets Sail: Ocean-Based Server Farms and International Law, 43 U. Conn. L. Rev. 709, 716-18 (2011). Thus, under Microsoft's understanding, certain information within the control of an American service provider would be completely unavailable to American law enforcement under the SCA.⁴

The practical implications thus make it unlikely that Congress intended to treat a Section 2703(a) order as a warrant for the search of premises located where the data is stored.

E. Principles of Extraterritoriality

The presumption against territorial application

provides that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none, Morrison v. National Australia Bank Ltd., 561 U.S. 247, __, 130 S. Ct. 2869, 2878 (2010), and reflect the "presumption that United States law governs domestically but does not rule the world," Microsoft Corp. v. AT & T Corp., 550 U.S. 437, 454 (2007).

Kiobel v. Royal Dutch Petroleum Co., __ U.S. __, __, 133 S. Ct. 1659, 1664 (2013). But the concerns that animate the presumption against extraterritoriality are simply not present here: an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical

⁴ Non-content information, opened e-mails, and unopened e-mails stored more than 180 days could be obtained, but only by means of a subpoena with notice to the target; unopened e-mails stored less than 180 days could not be obtained at all.

presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States. Many years ago, in the context of sanctioning a witness who refused to return from abroad to testify in a criminal proceeding, the Supreme Court observed:

With respect to such an exercise of authority, there is no question of international law, but solely of the purport of the municipal law which establishes the duty of the citizen in relation to his own government. While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States, the question of its application, so far as citizens of the United States are concerned, is one of construction, not of legislative power.

Blackmer v. United States, 284 U.S. 421, 437 (1932) (footnotes omitted). Thus, the nationality principle, one of the well-recognized grounds for extension of American criminal law outside the nation's borders, see Marc Rich, 707 F.2d at 666 (citing Introductory Comment to Research on International Law, Part II, Draft Convention on Jurisdiction With Respect to Crime, 29 Am. J. Int'l Law 435, 445 (Supp. 1935)), supports the legal requirement that an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation.

The cases that Microsoft cites for the proposition that there

is no authority to issue extraterritorial warrants are inapposite, since these decisions refer to conventional warrants. For example, in United States v. Odeh, 552 F.3d 157 (2d Cir. 2008), the Second Circuit noted that "seven justices of the Supreme Court [in United States v. Verdug-Urquidez, 494 U.S. 259 (1990)] endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches," id. at 169, and found that "it is by no means clear that U.S. judicial officers could be authorized to issue warrants for overseas searches," id. at 171. But Odeh involved American law enforcement agents engaging in wiretapping and searching a residence in Kenya. Id. at 159-60. The court held that while the Fourth Amendment's proscription against unreasonable search and seizure would apply in such circumstances, the requirement of a warrant would not. Id. at 169-71. Similarly, in Verdug-Urquidez, the Supreme Court held that a Mexican national could not challenge, on Fourth Amendment grounds, the search of his residence in Mexico by American agents acting without a warrant. 494 U.S. at 262-63, 274-75; id. at 278 (Kennedy, J., concurring); id. at 279 (Stevens, J., concurring). Those cases are not applicable here, where the requirement to obtain a section 2703(a) order is grounded in the SCA, not in the Warrant Clause.

Nor do cases relating to the lack of power to authorize intrusion into a foreign computer support Microsoft's position. In

In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013), the court rejected the Government's argument that data surreptitiously seized from a computer at an unknown location would be "located" within the district where the agents would first view it for purposes of conforming to the territorial limitations of Rule 41. Id. at 756-57. But there the Government was not seeking an SCA Warrant.

The Government [did] not seek a garden-variety search warrant. Its application request[ed] authorization to surreptitiously install data extraction software on the Target Computer. Once installed, the software [would have] the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.

Id. at 755. "In other words, the Government [sought] a warrant to hack a computer suspected of criminal use." Id. Though not "garden-variety," the warrant requested there was conventional: it called for agents to intrude upon the target's property in order to obtain information; it did not call for disclosure of information in the possession of a third party. Likewise, in United States v. Gorshkov, No. CR 00-550, 2001 WL 1024026 (W.D. Wash. May 23, 2001), government agents seized a computer in this country, extracted a password, and used it to access the target computer in Russia. Id. at *1. The court characterized this as "extraterritorial access"

to the Russian computer, and held that "[u]ntil the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment." Id. at *3. But this case is of even less assistance to Microsoft since the court did not suggest that it would have been beyond a court's authority to issue a warrant to accomplish the same result.⁵

Perhaps the case that comes closest to supporting Microsoft is Cunzhu Zheng v. Yahoo! Inc., No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2008), because at least it deals with the ECPA. There, the plaintiffs sought damages against an ISP on the ground that it had provided user information about them to the People's Republic of China (the "PRC") in violation of privacy provisions of the ECPA and particularly of the SCA. Id. at *1. The court found that "the alleged interceptions and disclosures occurred in the

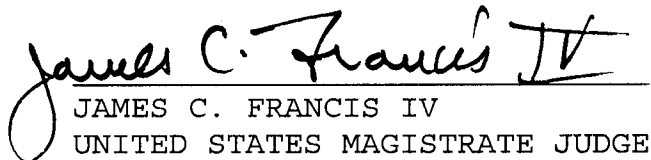
⁵ Microsoft argues that the Government itself recognized the extraterritorial nature of remote computer searches when it sought an amendment to Rule 41 in 2013. See Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division to Hon. Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) ("Raman Letter") at 4-5, available at <http://uscourts.gov/uscourts/RulesAndPolicies/>. But the proposed amendment had nothing to do with SCA Warrants directed to service providers and, rather, was intended to facilitate the kind of "warrant to hack a computer" that was quashed in In re Warrant to Search a Target Computer at Premises Unknown; indeed, the Government explicitly referred to that case in its proposal. Raman Letter at 2.

PRC," id. at *4, and as a result, dismissed the action on the ground that "[p]laintiffs point to no language in the ECPA itself, nor to any statement in the legislative history of the ECPA, indicating Congress intended that the ECPA . . . apply to activities occurring outside the United States," id. at *3. But this language, too, does not advance Microsoft's cause. The fact that protections against "interceptions and disclosures" may not apply where those activities take place abroad hardly indicates that Congress intended to limit the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas.

Conclusion

Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, Microsoft's motion to quash in part the warrant at issue is denied.

SO ORDERED.


JAMES C. FRANCIS IV
UNITED STATES MAGISTRATE JUDGE

Dated: New York, New York
April 25, 2014

Copies mailed this date:

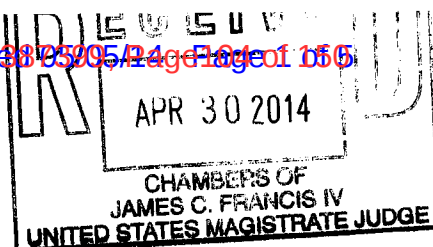
Guy Petrillo, Esq.
Nelson A. Boxer, Esq.
Petrillo Klein & Boxer LLP
655 Third Ave.
New York, NY 10017

Nancy Kestenbaum, Esq.
Claire Catalano, Esq.
Covington & Burling LLP
The New York Times Building
620 Eighth Ave.
New York, NY 10018-1405

James M. Garland, Esq.
Alexander A. Berengaut, Esq.
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401

Lorin L. Reisner, Esq.
Justin Anderson, Esq.
Serrin Turner, Esq.
Assistant U.S. Attorneys
One St. Andrew's Plaza
New York, NY 10007

DOC # 109



PETRILLO KLEIN & BOXER LLP

655 Third Avenue
22nd Floor
New York, NY 10017
Telephone: (212) 370-0331
www.pkbllp.com

Guy Petrillo
Direct Dial: (212) 370-0331
Cell: (646) 385-1479
gpetrillo@pkbllp.com

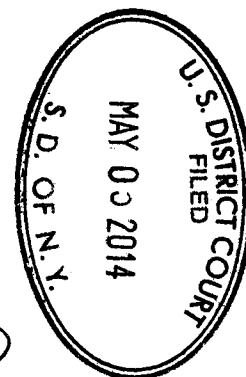
MEMO ENDORSED

USDC SDNY
DOCUMENT *UB*
ELECTRONICALLY FILED
DOC #: 11
DATE FILED: 5/5/14

April 30, 2014

BY HAND

Hon. James C. Francis IV
U.S. Magistrate Judge
Daniel Patrick Moynihan Courthouse
500 Pearl Street
New York, NY 10007-1312



M9-150

Re: *In the Matter of a Warrant to Search a Certain E-Mail Account
Controlled and Maintained by Microsoft Corporation, 13 Mag. 2814*

Dear Judge Francis:

In relation to the above referenced matter and on behalf of our client Microsoft Corporation ("Microsoft" or the "Company"), we respectfully submit this letter motion for a stay pending appeal with respect to the Court's Order ("Order") denying Microsoft's Motion ("Motion") To Vacate In Part An SCA Warrant Seeking Customer Information Located Outside the United States.

As discussed below, the standards for the issuance of a stay pending appeal are readily satisfied in this case given that the Court's ruling (i) addresses as a matter of first impression an interpretation of the warrant authority under the SCA as to which Microsoft will raise serious issues going to the merits of the appeal; (ii) could prejudice Microsoft because the Warrant calls for the seizure of email data stored in a foreign nation that has its own applicable data privacy laws; (iii) could further prejudice Microsoft because absent a stay, Microsoft's appeal might be deemed moot; (iv) appears not to involve an urgent criminal investigation; and (iv) implicates compliance by the United States with the MLAT regime.

A. Applicable Standards

The decision to enter a stay pending an interlocutory appeal falls within the discretion of the district court. *Nken v. Holder*, 556 U.S. 418, 433-34 (2009). In this Circuit, "[f]our criteria are relevant in considering whether to issue a stay of an order of a district court or an administrative agency pending appeal: the likelihood of success on the merits, irreparable injury if a stay is denied, substantial injury to the party opposing a stay if one is issued, and the public

James C. Francis IV
April 30, 2014

interest.” *United States v. Stein*, 452 F. Supp. 2d 281, 282-83 (S.D.N.Y. 2006) (quoting *Mohammed v. Reno*, 309 F.3d 95, 100 (2d Cir. 2002)); *see also* *Natural Res. Def. Council, Inc. v. U.S. Food & Drug Admin.*, 884 F. Supp. 2d 108, 122 (S.D.N.Y. 2012); *Hizam v. Clinton*, 11 CIV. 7693 (JCF), 2012 WL 4220498, at *3 (S.D.N.Y. Sept. 20, 2012) (citing, *inter alia*, *LaRouche v. Kezer*, 20 F.3d 68, 72-73 (2d Cir. 1994)).

“[This] test contemplates that a movant may be granted relief even if it demonstrates something less than a likelihood of success on the merits of its appeal.” *Sutherland v. Ernst & Young LLP*, 856 F. Supp. 2d 638, 640-41 (S.D.N.Y. 2012) (citing *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34-38 (2d Cir. 2010)). Specifically,

if movant shows ‘serious questions’ going to the merits of its appeal as well as irreparable harm, the stay may be granted if the balance of hardships ‘tips decidedly’ in favor of the moving party.

Id. at 640 (citing *Citigroup Global Mkts.*, 598 F.3d at 34-38). Furthermore, in balancing the equities, “it is helpful to consider whether the harm to the applicant if a stay were denied and the order appealed from reversed would outweigh the harm to the opponent if a stay were granted and the order appealed from upheld.” *Stein*, 452 F. Supp. 2d at 283 (citing *Mohammed*, 309 F.3d at 101 & n.10).

While the party seeking a stay “bears the burden of proving that a stay should be granted, and stays pending an appeal are only granted in limited circumstances[,]” *Liberty Synergistics, Inc. v. Microflo Ltd.*, No. 11-CV-523 (MKB), 2013 WL 101427, *1 (E.D.N.Y. Jan. 8, 2013) (citation and internal quotation marks omitted), all four factors are interrelated, meaning that “more of one excuses less of the other,” *United States v. N.Y.C. Bd of Educ.*, 620 F. Supp. 2d 413, 416 (E.D.N.Y. 2009). Thus, for example, the “probability of success that must be demonstrated is inversely proportional to the amount of irreparable injury plaintiff will suffer absent the stay.” *Mohammed*, 309 F.3d at 101 (alteration, citation, and internal quotation marks omitted).

B. Discussion

We respectfully submit that a stay of the Order pending appeal is amply justified in the circumstances of this case.

1. A Stay is Warranted Because Microsoft Raises Serious Questions Going to the Merits of the Appeal

As a matter of first impression, the Order directly addresses whether the warrant authorized under Section 2703(a) of the SCA permits the search and seizure of content email data stored outside the United States. The question addressed is an exceptionally important one, given the potential for data storage all over the globe and the existence of both U.S. and non-U.S. legal regimes affecting the rights of millions of email service customers. Indeed, as the Court notes in the opening quote of the Order, it issued its opinion in a contextual setting in which the

James C. Francis IV
April 30, 2014

combination of the nature of the electronic medium and its disregard for geographical boundaries throws the law into “disarray.” (Order at 1 (citation omitted).) In such a matter of first impression, a stay pending appeal is appropriate. *See Jock v. Sterling Jewelers, Inc.*, 738 F. Supp. 2d 445, 447 (S.D.N.Y. 2010) (that case was one of first impression added weight to the “serious questions” factor); *see also Pearce v. E.F. Hutton Grp., Inc.*, 828 F.2d 826, 829 (D.C. Cir. 1987) (noting that district court granted stay so appeals court could decide the issue when it was one of “first impression” and defendant would suffer “substantial harm” if a stay was not imposed and the district court was later reversed); *Project Vote/Voting for Am., Inc. v. Long*, 275 F.R.D. 473, 474 (E.D. Va. 2011); *Miller v. Brown*, 465 F. Supp. 2d 584, 596 (E.D. Va. 2006).

In addition, Microsoft’s appeal will raise a number of issues that we respectfully submit constitute serious questions going to the merits of the appeal, including but not limited to:

(i) Whether the Court’s first impression interpretation of Section 2703(a), including that the warrant provided for by this section is a hybrid instrument with subpoena-like qualities, is error, in view of the plain meaning of the statute, the canons of statutory construction, and the well-settled understanding of the term warrant in criminal procedure, and, relatedly, whether a warrant is a constitutionally significant court order that, as exemplified by the Warrant here, authorizes affirmative law-enforcement activity, whereas a subpoena to a third party is merely an order that authorizes no unilateral government action;

(ii) Whether the Court erred in ruling that email content data are located for purposes of the SCA in the place where the data are first viewed, as opposed to where they are stored;

(iii) Whether the Court misattributed to Congress an intention through the enactment of the SCA to permit the search and seizure of data stored outside the United States, given the settled rule of statutory construction that disfavors interpretations of congressional intent that contradict or undermine the United States’ international commitments; and relatedly, whether law enforcement efficiency can serve as a basis to find congressional intent inconsistent with such obligations; and

(iv) Whether the Court’s interpretation of the 2001 Amendments to the SCA and their implications is error.

2. A Balancing of the Equities Favors the Requested Stay

A balancing of the equities and the public interest here also favors the order of a stay pending appeal.

First, Microsoft would, in complying with the Warrant pursuant to the Order, encounter the likelihood that its appeal would be deemed moot. In such event, the Company – which would experience injury in this case by virtue of being compelled to act by an investigative tool that it argues is in part unauthorized by law – would effectively and irreparably lose its ability to challenge the Court’s ruling. Thus, this case falls outside of the class of cases in which the injury claimed by movant can be remedied through the process of appeal. *Providence Journal Co. v.*

James C. Francis IV
April 30, 2014

Fed. Bureau of Investigation, 595 F.2d 889, 890 (1st Cir. 1979) (“Appellants’ right of appeal here will become moot unless the stay is continued pending determination of the appeals. Once the documents are surrendered pursuant to the lower court’s order, confidentiality will be lost for all time. The status quo could never be restored.”); *see In re Agent Orange Prod. Liab. Litig.*, 804 F.2d 19, 20 (2d Cir. 1986) (per curiam) (stay of distribution of award challenged on appeal to avoid irreparable harm).

Second, the equities further favor Microsoft because the Order would require Microsoft to gather data from its data center in Ireland, which has its own data privacy protection regime.¹ Before the Warrant is deemed to control the resolution of any differences in the data privacy statutes of the United States and another nation, we respectfully submit that the interpretation of the SCA announced in the Order should be tested on appeal.

Third, with respect to potential prejudice to the government, Microsoft earlier agreed to preserve the evidence sought by the Warrant during the pendency of proceedings, including appeal. Also of relevance is that the government has not sought expedited proceedings before Your Honor and sought and received an extension of the briefing schedule, facts that strongly suggest that the matter to which the Warrant relates is not in furtherance of an urgent investigative matter.

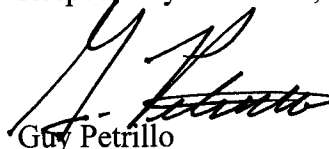
Concerning the public interest, there are strong reasons to stay enforcement of the Order pending appeal. In particular, national policy in the context of the comity of nations is at stake. The Order’s interpretation of the SCA’s warrant provision would permit the United States to ignore the MLAT process when it seeks through a warrant issued under the SCA to seize data stored in a facility in a foreign nation, and would do so arguably without a legislative determination that the United States should live by such a rule. It is manifestly in the public interest for an appellate court to determine whether the SCA incorporates a congressional determination to ensconce such a national policy in the law.

C. Conclusion

For all of the above-stated reasons, Microsoft respectfully seeks a stay of the Order pending appeal.

5/5/14
Application granted.
SO ORDERED.
James C. Francis IV
JCF

Respectfully submitted,


Guy Petrillo

¹ Data secrecy in Ireland is governed by The Data Protection Act of 1988 (as amended), which contains its own standards concerning nondisclosure obligations of “data processors.” *See* § 21(1).

James C. Francis IV
April 30, 2014

cc: AUSA Lorin Reisner
AUSA Justin Anderson
AUSA Serrin Turner
(by email)

Nancy Kestenbaum, Esq
James Garland, Esq.
Alexander Berengaut, Esq.
(by email)



U.S. Department of Justice

DOC # 114

United States Attorney
Southern District of New York

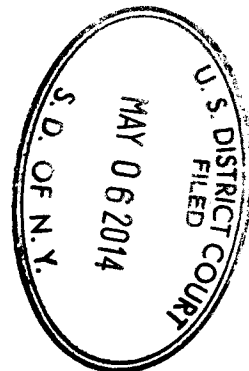
The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

May 2, 2014

BY ELECTRONIC MAIL AND HAND DELIVERY

Honorable James C. Francis
United States Magistrate Judge
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: **In re Search Warrant,**
No. 13 Mag. 2814, M9-150



Dear Judge Francis:

The Government respectfully submits this letter in response to the April 30, 2014 letter submitted by Microsoft Corporation ("Microsoft"), requesting a stay pending appeal of Your Honor's order denying Microsoft's motion to vacate. Although the Government does not oppose the entry of a stay, on the condition that Microsoft seeks its appeal promptly and without delay, the Government writes to correct a number of inaccuracies in the Microsoft April 30 letter.

First, Microsoft's compliance with the Stored Communications Act ("SCA") warrant at issue would not involve "seizure of email data stored in a foreign nation." (Microsoft Ltr. at 1). As explained in Your Honor's ruling, there is no such extraterritorial seizure and "the SCA does not implicate principles of extraterritoriality." (Slip op. at 12). It is uncontested that a Microsoft employee located in the United States can access, review, and produce the responsive materials. As the Government demonstrated and as the Court held, an SCA warrant functions similarly to a subpoena: it is served upon a provider inside the United States and requires the provider to produce the records at issue to the Government. It "does not involve government agents entering the premises of the [provider] to search its servers and seize the e-mail account in question" – and does not authorize projection of Government force abroad. (*Id.*) It has been the law for many decades that a company in the United States, served with a demand for the disclosure of documents in connection with a federal criminal investigation, is required to produce any responsive records in its possession, custody, or control – regardless of the location of that information. *See Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 564 (S.D.N.Y. 2002). Microsoft will not be prejudiced by producing records stored abroad in response to an SCA warrant any more than it would be prejudiced by doing so in response to a subpoena.

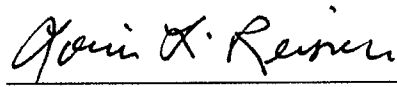
Hon. James C. Francis
May 2, 2014
Page 2 of 2

Second, this case does not implicate “compliance by the United States with the MLAT regime.” (Microsoft Ltr. at 1). The Government is not required to issue an MLAT to serve compulsory process on a domestic corporation. Microsoft’s position apparently is that any time a U.S. service provider stores documents abroad – even unknowingly, for example, by using a cloud storage service with servers in multiple countries (or possibly in no country) – the Government would be required to use an MLAT (or multiple MLATs) to obtain the documents, rather than by proceeding with compulsory process in accordance with Section 2703. That position does not square either with the law or with common sense.

Third, the Government does not believe that Microsoft stands to suffer any harm in the absence of a stay, or that any policy interests favor the entry of a stay. Nonetheless, the Government recognizes the importance of obtaining a definitive resolution of the questions raised by Microsoft’s motion in the absence of a mootness issue, in order to avoid successive challenges to future SCA warrants and the potential disruption to the criminal justice process. Accordingly, the Government is prepared to consent to a stay, on the condition that Microsoft seeks its appeal promptly and without any delay, so that this matter may proceed through the appropriate appeals process expeditiously.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 

LORIN L. REISNER
JUSTIN ANDERSON
SERRIN TURNER
Assistant United States Attorneys
(212) 637-1035

cc: Counsel of record (by email)

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #
DATE FILED: JUN 06 2014

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained by
Microsoft Corporation

REDACTED

Action Nos. 13-MAG-2814, M9-150

Declaration Of **REDACTED**

1. **REDACTED** declare as follows:

1. I am a Senior Compliance Manager for Microsoft Corporation in Ireland. I have worked for Microsoft since June 2010. In my current position, I am responsible for responding to legal orders for customer data that Microsoft receives from Irish law enforcement. I have personal knowledge of the facts stated in this declaration.

2. When Irish law enforcement authorities seek the content of customer emails stored on Outlook.com, Microsoft's free web-based email service, they generally follow a four-step process. By the "content of customer emails," I mean the body of the email and its subject line, as opposed to metadata about the email, such as the date and time it was sent.

3. First, Irish law enforcement authorities submit a legal request addressed to Microsoft Corporation in Redmond, WA, USA, for basic subscriber information about a specified Outlook.com account. These requests are submitted under Section 8(b) of the Data Protection Act of 1998, or under specific legislation pertaining to the investigation, such as the Child Trafficking and Pornography Act of 1998. Microsoft complies with valid requests from Irish law enforcement and produces this information.

4. Second, if Irish law enforcement wishes to obtain additional information about the account in question, they ordinarily will follow up with an additional request inquiring as to the location of the data -- *e.g.*, whether it is stored in our Dublin datacenter or elsewhere.

5. Third, if the email content data for the specified account is stored in the Dublin datacenter, Irish law enforcement will then obtain a warrant or court order for the data, as required under Irish law. Microsoft will not produce email content to Irish law enforcement that is stored outside of Ireland. For example, when Irish law enforcement has sought to obtain Microsoft user email content data stored in Microsoft datacenters located in the United States, I have referred them to the procedures available to them under United States-Ireland Mutual Legal Assistance Treaty.

6. Fourth, Irish law enforcement then arranges to serve me personally with a warrant or court order for the email content, which is generally directed both to Microsoft Corporation (in the United States) and to its Irish subsidiary. Under Irish law, I have seven days after receipt of the court order or warrant to produce the required customer content. During my tenure, we have always met the deadline for producing the requested data.

* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: 6/3/2014

REDACTED

Signed:

DOCUMENT
ELECTRONICALLY FILEDUNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained by
Microsoft Corporation

REDACTED

Action Nos. 13-MAG-2814, M9-150

Declaration Of Rajesh Jha

I, Rajesh Jha, declare as follows:

1. I am a Corporate Vice President at Microsoft Corporation. I have worked for Microsoft since 1990. I began as a software design engineer. I have worked on various products and services throughout my Microsoft career. In my current position, I am responsible for leading Microsoft's Outlook/Office 365 Shared organization within the Application & Services Group. In this capacity I lead development and service engineering for Microsoft's Office 365 enterprise and Outlook.com consumer services, among several other engineering responsibilities. Outlook.com is the successor to Hotmail, and to MSN email services (i.e. the service at issue in this case.) I also lead the Application & Services Group's engineering teams in Norway and China. I have a master's degree in computer science from the University of Massachusetts, Amherst and a bachelor's degree in computer science from Indian Institute of Technology, Madras (Chennai). I have personal knowledge of the facts stated in this declaration.

2. Cloud computing is the use of connected computers and network resources to enable providers such as Microsoft, Google and Amazon to deliver computing resources to users as a service over the Internet. These services made available to the general public (or "public cloud services") can be operated at tremendous scale and provide users with the resources to run

applications, store data, or perform other computing tasks. Historically, businesses, governments and educational institutions were required to make substantial investments in their own computing hardware, software and infrastructure in order to provide their users with such computing capabilities. With the development, availability and adoption of public cloud services, the need for such investment is increasingly becoming unnecessary. Cloud services also ensure that customers always have the most up-to-date computing resources available.

3. This shift in computing has been transformative. It provides tremendous efficiencies to traditional computing-intensive enterprises by enabling them to invest resources in core purposes, as opposed to IT infrastructure. It also unleashes incredible productivity opportunities for enterprises that previously could not afford, or were otherwise unable to make, the investments in information technology that have generally been required. It has also provided tremendous value to consumers – who are able to use cloud computing to obtain free or inexpensive use of vast computer resources to access services, communicate with one another, and store their personal data.

4. Microsoft offers several enterprise public cloud services used by businesses, governments and educational institutions worldwide. These include, but are not limited to, Office 365 (a suite of software applications for commercial productivity services, including email and word processing), Microsoft Azure (platform and infrastructure resources to build, deploy and manage applications and services globally), and CRM Online (sales productivity and resource management services). Microsoft also offers consumer cloud services such as Outlook.com, which provides email and instant message communications to millions of users throughout the world.

5. Microsoft's enterprise cloud service offerings are made available in 100+ countries through a regionally segmented public cloud. This means that Microsoft's public cloud is segmented into regions, and most customer data (e.g. email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located. This is the most scalable, reliable and cost effective approach. We believe other large enterprise cloud vendors have taken a similar approach. Microsoft stores data for its major enterprise public cloud services in data centers throughout the world in North America, Latin America, Europe and Asia. Some of the countries in which we currently host customer data include the United States, Ireland, the Netherlands, Japan and Brazil. This regional implementation is driven by engineering and business capabilities and constraints, as well as key imperatives such as optimizing for performance and communications latency minimization to deliver outstanding user experiences. [REDACTED]

[REDACTED]

6. Microsoft's global datacenter footprint for its enterprise and consumer cloud services is one of the largest in the world, and growing rapidly to accommodate what we expect will be growing customer demand for our cloud services. We currently manage over one million server computers in our datacenters worldwide, in over 100 discrete leased and owned datacenter facilities, spread over 40 countries. Further, it is conceivable that to accommodate the broader shift to cloud computing, each of these numbers could double over the next several years. These facilities host more than 200 online services, used by over 1 billion customers and over 20 million businesses worldwide.

7. The transition to the cloud by consumers and enterprises worldwide is accelerating at a rapid pace. Consumers increasingly store pictures, video, communications and private documents in the cloud, and access cloud computing services as part of their everyday life. Businesses, governments and educational institutions are increasingly taking critical dependencies on public cloud computing solutions, and shifting their information technology investments to such offerings. Based on industry and analyst data, we believe public cloud services will grow significantly over the coming years, and at a much higher rate than the information technology industry as a whole. In 2013, International Data Corporation (IDC) forecasted worldwide spending on public cloud services to reach almost \$59 billion in 2014, with slightly less than half from outside of the United States. IDC also forecasted that information technology industry spend on public cloud services outside of the United States will be approximately \$60 billion in 2017. Further, growth of cloud adoption outside the United States is expected to surpass domestic growth, and public cloud spending outside of the United States will account for more than 55% of worldwide public cloud spending by 2017. This tremendous growth is fueled by the efficiencies and economic benefit that cloud computing promises. Relative to traditional information technology spend by enterprises, cloud services are estimated to save customers as much as 30% to 40% per year.

8. In the year since disclosures by Edward Snowden regarding surveillance practices by the United States Government, Microsoft partners and enterprise customers around the world and across all sectors have raised concerns about the United States Government's access to customer data stored by Microsoft. These concerns relate not only to the actual and perceived practices of the National Security Agency that have been described following the disclosures by Edward Snowden, but there is also clearly a heightened concern, as a general matter, about

United States government access to customer data stored in data centers located outside of the United States that are operated by United States cloud service providers. The notion of United States government access to such data – particularly without notice to the customer – is extremely troubling to our partners and enterprise customers located outside of the United States.

9. These concerns of our partners and customers located outside of the United States have manifested themselves in a number of ways. The concerns are often a substantive topic of discussion in briefings or contract negotiations, and they create friction in the sales process and have a chilling effect on the business. Some customers have delayed a transition to cloud services until the environment around these issues is more settled. Other customers have chosen to not purchase public cloud services from Microsoft at all, and have instead opted for a non-cloud solution. Both of the foregoing result in customers maintaining the status quo of an aging, uncompetitive, less secure and more expensive information technology infrastructure. Customers have also acquired cloud services from a provider based outside of the United States that is perceived as not being subject to United States jurisdiction.

10. Some of these customers referred specifically to the decision in this case by Magistrate Judge Francis as a basis for concern about the United States Government's access to customer data. Although this case involves consumer cloud services, namely Outlook.com email services, many of our partners and enterprise customers (e.g. business and foreign government enterprises) see the U.S. government's unilateral approach to obtaining private data in this case as a threat to the privacy and protection of enterprise data as well. This concern is greatly reduced when the U.S. government is perceived to be acting in cooperation with their counterparts in other governments (thereby ensuring local enterprises that they remain entitled to the privacy and procedural protections of their own governments).

11. This perception of unilateral United States Government access to customer data situated in data centers outside of the United States will in my belief have a substantive negative impact on our public cloud business model. Transition to the public cloud, whether by enterprises or consumers, requires trust in the cloud service provider to deliver a secure and reliable cloud service. An absolute imperative is that the cloud service provider protect the integrity and privacy of its customers' data. Microsoft has made significant investments in the security and reliability of its cloud services to protect customer data. Microsoft has also made significant capital investments in the establishment of data centers situated regionally throughout the world to address customer expectations relative to the location of data storage. Our customers around the world, through their decision to move to our cloud services, have demonstrated that they trust Microsoft and have confidence in the technical and operational safeguards we deploy to protect their data. However, in the wake of the Edward Snowden disclosures and the decision in this case by Magistrate Judge Francis, enterprises and consumers have also clearly indicated that the perception of unilateral government access to their data is undermining that trust and confidence.

12. Ultimately, these concerns will impact the ability of Microsoft and other United States cloud providers to remain competitive in the global marketplace. To the extent foreign enterprises and consumers perceive that their data entrusted to United States cloud service providers, even when that data resides outside of the United States, is subject to unilateral access by the United States government, there will be increasing demand for national public clouds operated by cloud service providers perceived as not subject to United States Government jurisdiction. Microsoft and other U.S. companies will lose market share, and as a result, the

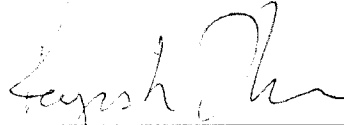
compelling opportunity that cloud computing offers to our customers through cost savings, productivity gains, and access to the latest information technologies will not be fully realized.

* * *

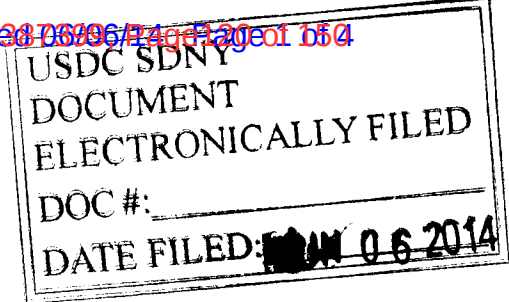
Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: June 5, 2014

Signed:



Rajesh Jha



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained by
Microsoft Corporation

Action Nos. 13-MAG-2814, M9-150

DECLARATION OF MICHAEL MCDOWELL

I, **MICHAEL MCDOWELL**, declare as follows:

1. I am a Senior Counsel at the Bar of Ireland, having been called to the Bar in 1974 and to the Inner Bar in 1987. I was Attorney General of Ireland from 1999 to 2002, Minister of Justice, Equality and Law Reform from 2002 to 2007, and Deputy Prime Minister from 2006 to 2007. I left government service in 2007, and I am now in practice as a Senior Counsel in the Irish High and Supreme Courts. I have been engaged by Microsoft as an independent expert to opine on the issues raised in this case.

2. As Attorney General of Ireland, I was legal advisor to the Irish Government during the negotiation and implementation of the Mutual Legal Assistance Treaty Between the United States and Ireland, signed January 18, 2001 (the "U.S.-Ireland MLAT"). In 2003, the European Union and the United States entered a separate agreement on mutual assistance, which was subsequently applied in relation the U.S.-Ireland MLAT. The MLA treaties between Ireland and the United States were intended by the treaty signatories to serve as the means for law enforcement authorities in the respective countries to obtain evidence located in the other treaty party.

3. In 2008, Ireland enacted the Criminal Justice (Mutual Assistance) Act, 2008, to provide for procedures for responding effectively to requests made under these

international agreements (the “2008 Act”). Pursuant to these procedures, qualified U.S. authorities are able to seek the assistance of the Irish state in obtaining evidence located in Ireland that may be relevant to criminal investigations or proceedings in the United States.

4. Requests for assistance are evaluated by Ireland’s Central Authority for Mutual Assistance (the “Central Authority”), which is part of the Department of Justice and Equality. Provided that the assistance requested by the United States would comply with the standards established in the 2008 Act — *e.g.*, compliance would not prejudice Irish security or sovereignty — the Central Authority will execute the request. Refusal by Ireland to execute a proper request duly made for assistance from U.S. authorities is very uncommon.

5. To fulfill a request for assistance, the Central Authority forwards the request to An Garda Síochána — Ireland’s national police service. Where the information sought is email content, An Garda Síochána apply on an *ex parte* basis for a search warrant or order from an Irish district court judge.

6. If the application submitted to the court satisfies the legal standards set out in the 2008 Act, the judge then forthwith issues a warrant authorising An Garda Síochána to conduct a search of the places or persons identified in the application, or an order requiring persons (including webmail service providers) to produce the requested materials. The police may then execute the warrant, or, in the case of an order, serve it upon the appropriate recipient.

7. Webmail service providers in Ireland must comply with any warrant or order issued by a district court judge. To obstruct the Garda Síochána’s execution of such process is a criminal offense that carries punishment of six months’ imprisonment or a €2500 fine.

8. The 2008 Act procedures are a highly effective means of realizing the MLA treaties' objectives. Ireland rarely refuses requests for information made under the treaties, as noted above, and the current MLAT procedures for fulfilling these requests are efficient and well-functioning.

9. In the present case, I understand that U.S. law enforcement seeks email content stored on Microsoft's servers in Dublin, Ireland. The aforementioned treaties and procedures were designed to apply under precisely these circumstances. The U.S. government should therefore obtain the evidence it seeks through the MLA treaties.

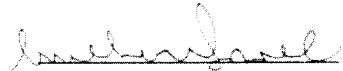
10. Ireland's Data Protection Acts, 1998 to 2003, highlight its sovereign interest in guarding against the exercise of foreign law enforcement activities within its borders by any means other than the applicable MLA treaties. As a sovereign state and member state of the European Union, Ireland's data protection law, in accordance with EU Directives and the Council of Europe Convention on Data Protection, requires Ireland to protect the rights of data subjects in relation to data located in the jurisdiction of Ireland. Absent certain particular exceptions, disclosure to a third party of such data (*i.e.*, data that is stored and processed in Ireland) is only lawful pursuant to orders made by the Irish courts. And in such cases, any disclosure to a third party on the grounds of "legal obligation" or that it is "necessary for the administration of justice" is only lawful where such disclosure is required or mandated by reference to Irish law and subject to the jurisdiction and control of the Irish courts.

* * *

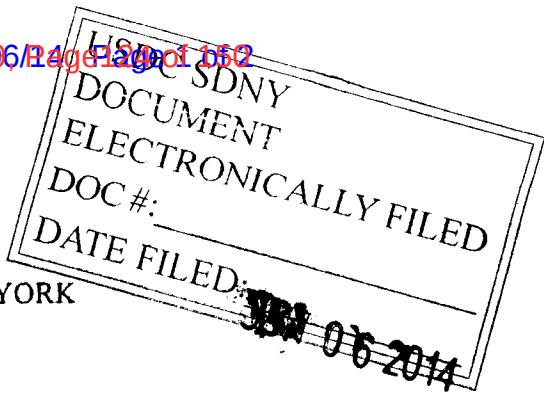
I declare under penalty of perjury under the laws of the United States of America
that the foregoing is true and correct.

Executed on 5 June 2014.

Signed:



Michael McDowell



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained
By Microsoft Corporation

REDACTED

Action Nos. 13-MAG-2814, M9-150

Supplemental Declaration Of REDACTED

I, REDACTED declare as follows:

1. I am a Lead Program Manager for Microsoft Corporation. I am responsible for managing the storage “backend” for Outlook.com, which is the current Internet domain name for Microsoft’s web-based customer email service. This declaration supplements my declaration of December 17, 2013, and provides additional information regarding Microsoft’s practices for storing Outlook.com user information. I have personal knowledge of the facts stated in this declaration.

2. When a user accesses Outlook.com through his or her web browser (*e.g.*, Internet Explorer, Safari, Firefox, Chrome), the user connects to a login page where the user must enter his or her username and password. REDACTED

REDACTED

3. REDACTED

REDACTED

4.

REDACTED

REDACTED

5.

REDACTED

REDACTED

6. Microsoft only has access to Outlook.com user content stored on its servers, and cannot access copies of Outlook.com user content that may be stored on an individual user's computer. For example, if a user accesses Outlook.com through a web browser, the browser may temporarily store a local cache of the user's content and non-content information. Because those copies are stored on the user's computer and not on Microsoft's servers, Microsoft has no access to that information.

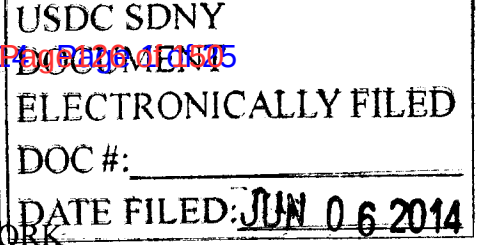
* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: 5/29/2014

REDACTED

Signed:



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain
E-Mail Account Controlled and Maintained By
Microsoft Corporation

Case Nos. 13-MAG-2814; M9-150

CLAIRE CATALANO, pursuant to 28 U.S.C. § 1746, declares as follows under
penalties of perjury:

1. I am an attorney duly admitted to practice before this Court, and an associate of the firm Covington & Burling LLP, counsel for Microsoft Corporation.
2. I submit this declaration in support of the above-referenced motion.
3. I attach as Exhibit 1 a true and correct copy of an Email from Christopher B. Harwood, Assistant United States Attorney, United States Attorney's Office for the Southern District of New York, to Nathan Wessler, American Civil Liberties Union, dated April 19, 2013, *available at* <http://www.aclu.org/files/pdfs/email-content-foia/EOUSA%20docs/EOUSA%20response%20email%204.19.13.pdf>.
4. I attach as Exhibit 2 a true and correct copy of an article titled "How Brazil and the EU Are Breaking the Internet," published by Forbes on May 19, 2014, *available at* <http://www.forbes.com/sites/elisugarman/2014/05/19/how-brazil-and-the-eu-are-breaking-the-internet/>.
5. I attach as Exhibit 3 a true and correct copy of a Letter from Sophie in't Veld, Member of the European Parliament, to Viviane Reding, Vice-President of the European Commission, dated April 28, 2014, *available at* <http://www.statewatch.org/news/2014/may/ep->

letter-to-Vice-President-Reding-on-extraterritorial-jurisdiction-US-Stored-Communications-Act-unsigned.pdf.

6. I attach as Exhibit 4 a true and correct copy of an article titled “Microsoft ‘must release’ data held on Dublin server,” published by the British Broadcasting Corporation on April 29, 2014, *available at* <http://www.bbc.com/news/technology-27191500>.

7. I attach as Exhibit 5 a true and correct copy of a Memorandum from the European Commission titled “Restoring Trust in EU-US data flows – Frequently Asked Questions,” dated November 27, 2013, *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

Dated: June 6, 2014
New York, NY



Claire Catalano, Esq.

EXHIBIT 1

Nathan Wessler

From: Harwood, Christopher (USANYS) <Christopher.Harwood@usdoj.gov>
Sent: Friday, April 19, 2013 4:59 PM
To: Nathan Wessler
Subject: ACLU v. DOJ, No. 12-4677

Dear Nate,

Pursuant to paragraphs 1 and 2 of the parties' stipulation dated March 22, 2013, EOUSA was required to ask the current Criminal Chiefs in the United States Attorneys' Offices for the Southern District of New York, the Eastern District of New York, the Northern District of Illinois, the Northern District of California, the Eastern District of Michigan, and the Southern District of Florida whether, since *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), their respective Offices have ever authorized a request to a court for access to the contents of a person's private electronic communications for law enforcement purposes without a warrant or on a standard less than probable cause. By April 19, 2013, EOUSA was required to inform ACLU, in writing, how each of the relevant Criminal Chiefs responded.

I write on behalf of EOUSA to report that each of the Criminal Chiefs responded, "no."

Please let me know if you have any questions.

Chris

Christopher B. Harwood
Assistant United States Attorney
Southern District of New York
86 Chambers Street
New York, NY 10007
Telephone: (212) 637-2728
Facsimile: (212) 637-2786
Email: christopher.harwood@usdoj.gov

EXHIBIT 2



Eli Sugarman Contributor

I write about technology policy issues.

Opinions expressed by Forbes Contributors are their own.

TECH 5/19/2014 @ 9:38AM 5,097 views

How Brazil and the EU Are Breaking the Internet

[Comment Now](#)

The Internet is a global and borderless network with nearly 3 billion users, but individual governments are undermining the Net's foundation by extending the reach of their local laws to Internet companies worldwide. Europe's highest court shocked the technology industry last week by ruling that Internet search engines must self-censor search results in certain circumstances to comply with the EU's data privacy law. And last month, Brazil foisted different data privacy rules on any Internet company with one or more Brazilian users (regardless of the company's geographic location). This ever-growing thicket of Internet regulations threatens the free and open Internet as we know it.

Last month, on April 24, 2014, Brazilian President Dilma Rouseff signed into law the Marco Civil Da Internet, touted as the Internet "Magna Carta." It contains several business-friendly provisions that ensure network neutrality and protect companies from intermediary liability (i.e. websites are generally not liable for third party content posted on their sites). But it also obliges Internet businesses – ranging from social media sites to online marketplaces – to follow certain privacy rules, and also mandates how they store and share users' information. Most importantly, the law explicitly applies to any company anywhere that has at least one Brazilian user, has servers located in Brazil, or operates an office there, or effectively, all Internet companies on Earth.



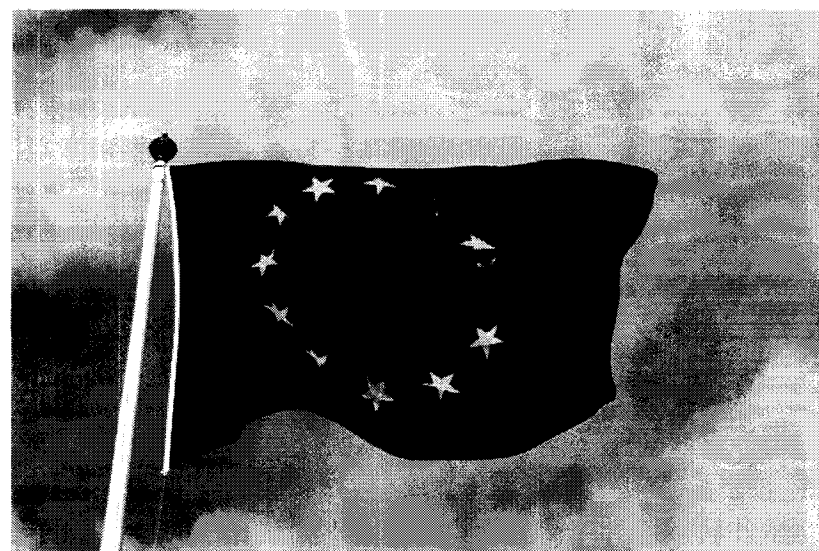
Manifestação durante o Fórum: o marco civil da internet - Campus Party Brasil 2013, 30/01/2013 - Foto: Cristiano Sant'Anna/Indicefoto

Marco Civil da Internet (Photo credit: Manuela d'Ávila)

Failure to comply can result in fines of up to ten percent of Brazil-origin revenues or service blockage in Brazil. Once the law enters into effect next month, a Silicon Valley-based firm could, for example, be penalized for complying with U.S. data protection laws that conflict with the Marco Civil. The law provides no guidance – or options – for the many transnational companies that will face competing regulations.

Last week, on May 13, 2014, the European Court of Justice (ECJ) even more problematically ruled that Internet search engines – such as Google or Microsoft – must remove links to third party content from search results where an individual's privacy interest outweighs the public's need for that information. This so-called “right to be forgotten” was articulated in response to a Spanish citizen's suit against Google for not removing links to old (but at the time accurate) Spanish newspaper announcements that he claimed violated his privacy.

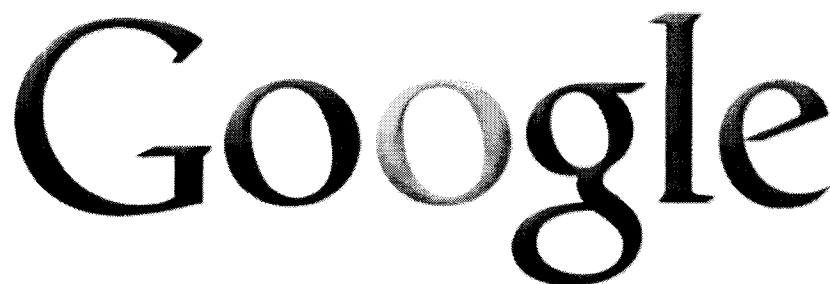
Despite vocal criticism of the ECJ's dubious legal reasoning, Google and Microsoft must now design internal procedures to translate the ruling into an actual process to evaluate and implement users' removal requests. At what point does an old bankruptcy proceeding become private information? Is the standard different if the information pertains to a criminal conviction? What if the subject of the information is a celebrity? And what if anything happens if a user runs for public office after having the links taken down, effectively masking their past from voters? An ex-politician who previously misbehaved in office and a convicted pedophile have already petitioned Google to remove links to news articles about them.



EU Flag (Photo credit: MPD01605)

These are but a few of questions that search engines will confront, each of which will require new systems, immense legal and technical expertise, and other resources. Moreover, the costs to technology companies will increase as the number of different rules increases due to each EU member state interpreting the ruling differently. Given the vagueness of the ECJ decision, this is all but assured, and could even lead to venue shopping where individuals seek out the most favorable country within Europe to bring their complaint.

The task now falls to the EU's 28 member state data privacy regulators and courts to interpret and implement the ruling. While the reach of the ruling is unclear – unlike the flagrant extraterritorial ambitions of Brazil's Internet Law – the ECJ did affirm that the fact that Google's servers being housed outside of Spain does not excuse the company from compliance. Still, it remains unclear if the ruling applies only to searches carried out in Europe or also searches made outside Europe but about EU citizens.



Google Logo (Photo credit: Wikipedia)

It is not difficult to imagine a scenario in which searches conducted from Brazil, for example, include links to "private" information that would be censored from search results in Europe. Will the EU attempt to apply its data privacy rules to protect information about EU citizens regardless of where the

search is conducted? If so, this would in turn potentially violate American free speech protections if the search was conducted in the United States. In short, the quagmire of likely resultant legal conflicts is hard to exaggerate.

As more and more countries follow the EU and Brazil's lead, Internet companies will have to navigate an increasingly bewildering web of conflicting Internet rules. Technology investment may flee some jurisdictions as administrative burdens increase; this is especially likely in smaller markets where compliance costs are more difficult to justify. Governments must resist the urge to apply their laws extra-territorially because doing so inevitably weakens the Internet. For the network of networks to survive, it must retain its fundamentally international foundation and not be carved up by short-sighted local laws.

This article is available online at: <http://onforb.es/1j2gldz>

2014 Forbes.com LLC™ All Rights Reserved

EXHIBIT 3

Brussels, 28 April 2014

Dear Vice-President Reding,

On Friday 25 April 2014, a US federal judge ruled that search warrants issued by US law enforcement authorities on the basis of the US Stored Communications Act extend to overseas email accounts.¹ This ruling again confirms that US authorities are able to obtain personal data of European citizens stored on EU territory. Does the Commission think that companies complying with such a warrant of a third country would be in breach of European and national data protection law?

Furthermore, how does the Commission assess this ruling of the US federal judge, and the impact of the US extraterritorial jurisdiction on the communications of European citizens? How does the Commission assess the impact of US extraterritorial jurisdiction on transatlantic agreements such as mutual legal assistance treaties, the EU US Passenger Name Record Agreement, the EU US TFTP Agreement, the Safe Harbour programme and the EU US umbrella agreement which is currently being negotiated?

Is the Commission aware of any other third country, for instance the Russia, exerting extraterritorial jurisdiction over personal data stored on European territory? How would the Commission respond to a breach in the protection of personal data on European soil through the extraterritorial jurisdiction of any other third country?

Has the Commission asked the US authorities for clarification? If not, why not? How is the Commission going to assure the European citizens that their personal data are protected against extraterritorial jurisdiction of third countries?

I urgently request the Commission to take serious steps in order to avoid any such violation of the European citizens' fundamental rights.

Kind regards,

Sophie in 't Veld

¹ Reuters, 25 April 2014, *U.S. judge rules search warrants extend to overseas email accounts*, link: <http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425>

EXHIBIT 4

PIN BBC TO YOUR TASKBAR BY DRAGGING THIS ICON  TO THE BOTTOM OF THE SCREEN

Close

BBC NEWS

TECHNOLOGY

29 April 2014 Last updated at 05:18 ET

Microsoft 'must release' data held on Dublin server

A judge in the US has ordered Microsoft to hand over a customer's emails, even though the data is held in Ireland.

The company had attempted to challenge the search warrant on the basis that the information was stored exclusively on computer servers outside the US.

Microsoft **previously said it planned** to offer business and government clients control over where their data resided.

This followed concerns about data privacy raised by whistleblower Edward Snowden's leaks about US spying.

But the ruling potentially undermines that pledge.

The judge said warrants for online data were different to other warrants.

The search warrant, which was issued to Microsoft by US authorities, sought information associated with a member of the public's email account including their name, credit card details and contents of all messages.

Microsoft said it would continue to oppose the release of the Dublin-stored data.

"This is the first step toward getting this issue in front of courts that have the authority to correct the government's longstanding views on the application of search warrants to content stored digitally outside the United States," it said.

'Government disagrees'

Judge James Francis in New York said that this was true for "traditional" warrants but not for those seeking online content, which are governed by federal law under the Stored Communications Act.

He said the warrant should be treated more like a subpoena for documents. Anyone issued with a subpoena by the US must provide the information sought, no matter where it was held, he said.

Law enforcement efforts would be seriously impeded and the burden on the government would be substantial if they had to co-ordinate with foreign governments to obtain this sort of information from internet service providers such as Microsoft and Google, Judge Francis said.

In a blog post, Microsoft's deputy general counsel, David Howard, said: "A US prosecutor cannot obtain a US warrant to search someone's home located in another country, just as another country's prosecutor cannot obtain a court order in her home country to conduct a search in the United States.

"We think the same rules should apply in the online world, but the government disagrees."

A new data-protection law, currently being drafted by the European Union, aims to make sure companies no longer share European citizens' data with authorities of another country, unless explicitly allowed by EU law or an international treaty.

In response to the ruling in the US, Mina Andreeva, European Commission spokeswoman for justice, fundamental rights and citizenship, told the BBC: "The commission's position is that this data should not be directly accessed by or transferred to US law enforcement authorities outside formal channels of co-operation, such as the mutual legal assistance agreements or sectoral EU-US agreements authorising such transfers.

"Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations."

Ms Andreeva also said that "the European Parliament reinforced the principle that companies operating on the European market need to respect the European data protection rules - even if they are located in the US."

Earlier this year German Chancellor Angela Merkel proposed building up a European communications network to help improve data protection and avoid emails and other data automatically passing through the United States.

Both of these actions were prompted by allegations of mass surveillance by the US National Security Agency.

Microsoft is hoping for a review of the decision from a federal district judge.

More Technology stories



[China criticises Windows 8 security](#)

[\[/news/technology-27712908\]](#)

Microsoft's Windows 8 is branded a threat to China's cybersecurity in a state-backed news report.

[Apple in row over HealthKit name](#)

[\[/news/technology-27713242\]](#)

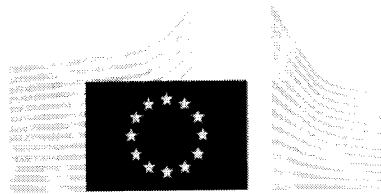
[Tinder introduces photo sharing](#)

[\[/news/business-27720930\]](#)



BBC © 2014 The BBC is not responsible for the content of external sites. Read more

EXHIBIT 5



EUROPEAN COMMISSION

MEMO

Brussels, 27 November 2013

Restoring Trust in EU-US data flows - Frequently Asked Questions

What is the Commission presenting today?

Today the European Commission has set out actions to be taken in order to restore trust in data flows between the EU and the U.S., following deep concerns about revelations of large-scale U.S. intelligence collection programmes, which have had a negative impact on the transatlantic relationship.

The Commission's response today takes the form of:

1. **A strategy paper (a Communication) on transatlantic data flows** setting out the challenges and risks following the revelations of U.S. intelligence collection programmes, as well as the steps that need to be taken to address these concerns;
2. **An analysis of the functioning of 'Safe Harbour'** which regulates data transfers for commercial purposes between the EU and U.S.;
3. **A factual report on the findings of the EU-US Working Group** on Data Protection which was set up in July 2013;
4. A **review** of the existing agreements on **Passenger Name Records (PNR)** see [MEMO/13/1054](#)),
5. As well as a **review** of the **Terrorist Finance Tracking Programme (TFTP)** regulating data exchanges in these sectors for law enforcement purposes see [MEMO/13/1164](#)).

In order to maintain the continuity of data flows between the EU and U.S., a high level of data protection needs to be ensured. The Commission today calls for action in six areas:

1. A swift adoption of the **EU's data protection reform**
2. Making **Safe Harbour** safe
3. Strengthening data protection safeguards in the **law enforcement** area
4. Using the existing **Mutual Legal Assistance** and Sectoral agreements to obtain data
5. Addressing European concerns in the on-going **U.S. reform** process
6. Promoting **privacy standards internationally**

1. The EU's Data Protection Reform: the EU's response to fear of surveillance

How will the EU data protection reform address fears of surveillance?

The EU data protection reform proposed by the Commission in January 2012 (IP/12/46) provides a key response as regards the protection of personal data. Five components of the proposed reform package are of particular importance.

1. **Territorial scope:** the EU data protection reform will ensure that non-European companies, when offering goods and services to European consumers, respect EU data protection law. The fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility.
2. **International transfers:** the proposed Regulation establishes clear conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard individuals' rights to a high level of protection, are met. The European Parliament, in its vote of 21 October, has even proposed to strengthen these conditions.
3. **Enforcement:** the proposed rules provide for dissuasive sanctions of up to 2% of a company's annual global turnover (the European Parliament has proposed to increase the maximum fines to 5%) to make sure that companies comply with EU law.
4. **Cloud computing:** the Regulation sets out clear rules on the obligations and liabilities of data processors such as cloud providers, including on security. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.
5. **Law Enforcement:** the data protection package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

Next Steps: The proposed data protection Regulation and Directive are currently being discussed by the European Parliament and the Council of Ministers. The European Parliament in a vote on 21 October gave its strong backing to the Commission's proposals so that the Parliament is ready to enter negotiations with the second chamber of the EU legislature, the Council of the European Union. European heads of state and government also underlined the importance of a "timely" adoption of the new data protection legislation at a summit on 24 and 25 October 2013. The Commission would like to conclude the negotiations by spring 2014.

2. Making Safe Harbour safer

What is the Safe Harbour Decision?

The 1995 EU Data Protection Directive sets out rules for transferring personal data from the EU to third countries. Under these rules, the Commission may decide that a non-EU country ensures an "adequate level of protection". These decisions are commonly referred to as "adequacy decisions".

On the basis of the 1995 Data Protection Directive, the European Commission, on 26 July 2000, adopted a Decision (the "Safe Harbour decision") recognising the "Safe Harbour Privacy Principles" and "Frequently Asked Questions", issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of personal data transfers from the EU.

As a result, the Safe Harbour decision allows for the free transfer of personal information for commercial purposes from companies in the EU to companies in the U.S. that have signed up to the Principles. Given the substantial differences in privacy regimes between the EU and the U.S., without the Safe Harbour arrangement such transfers would not be possible.

The functioning of the Safe Harbour arrangement relies on commitments and **self-certification** of the companies which have signed up to it. Companies have to sign up to it by notifying the U.S. Department of Commerce while the U.S. Federal Trade Commission is responsible for the enforcement of Safe Harbour. **Signing up to these arrangements is voluntary, but the rules are binding for those who sign up.** The fundamental principles of such an arrangement are:

- Transparency of adhering companies' privacy policies,
- Incorporation of the Safe Harbour principles in companies' privacy policies, and
- Enforcement, including by public authorities.

A U.S. company that wants to adhere to the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Principles and actually comply with the Principles, as well as (b) self-certify, meaning it has to declare to the U.S. Department of Commerce that it is in compliance with the Principles. The self-certification must be resubmitted on an annual basis.

The U.S. Department of Commerce and the U.S. Federal Trade Commission are responsible for the enforcement of the Safe Harbour scheme in the U.S.

How many companies are using it?

By late-September 2013, the Safe Harbour had a membership of **3246 companies** (an eight-fold increase from 400 in 2004).

Why is Safe Harbour relevant to surveillance?

Under Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security, the question has arisen whether the large-scale collection and processing of personal information under U.S. surveillance programmes is necessary and proportionate to meet the interests of national security. Safe Harbour acts as a conduit for the transfer of the personal data of EU citizens from the EU to the U.S. by companies required to surrender data to U.S. intelligence agencies under the U.S. intelligence collection programmes.

How would a review of Safe Harbour work in practice?

Legally speaking, the European Commission is in charge of reviewing the Safe Harbour Decision. The **Commission may maintain the Decision, suspend it or adapt it** in the light of experience with its implementation. This is in particular foreseen in cases of a systemic failure on the U.S. side to ensure compliance, for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role, or if the level of protection provided by the Safe Harbour Principles is overtaken by the requirements of U.S. legislation.

What is the European Commission proposing today with regards to Safe Harbour?

On the basis of a thorough analysis published today and consultations with companies, the European Commission is **making 13 recommendations to improve the functioning of the Safe Harbour scheme**. The Commission is calling on U.S. authorities to identify remedies by summer 2014. The Commission will then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations.

The 13 Recommendations are:

Transparency

1. Self-certified companies should publicly disclose their privacy policies.
2. Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme.
3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.
4. Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.

Redress

5. The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider.
6. ADR should be readily available and affordable.
7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. Following the certification or recertification of companies under Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).
9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.
10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.
11. False claims of Safe Harbour adherence should continue to be investigated

Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.
13. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

Relatively transparent information in this respect is provided by some European companies in Safe Harbour. For **example Nokia**, which has operations in the U.S. and is a Safe Harbour member provides a following notice in its **privacy policy**: "*We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate.*"

What are examples of the way in which Safe Harbour functions?

The Safe Harbour scheme allows for the provision of solutions for transfers of personal data in situations where other tools would not be available or not practical.

Orange France is using the cloud computing services of Amazon U.S. for the purposes of data storage. In order for the personal data of Orange France customers to be transferred outside the EU, Amazon U.S. subscribes to the Safe Harbour Principles, which is an alternative to a specific contractual arrangement between the two companies regarding the treatment of personal data transferred to the U.S.

For a global company, such as **Mastercard, based in the U.S.** but with a large number of clients in the EU, in order to channel the very large amount of personal data involved in its operations, it cannot have recourse to Binding Corporate Rules as they apply only to transfers within one corporate group. Transfers based on contracts would not work either because thousands would be needed, with different financial institutions. The Safe Harbour scheme offers the flexibility such a global organisation needs for its operations, while permitting the free flow of data outside of the EU, subject to the respect of the Safe Harbour Principles.

3. Strengthening data protection safeguards in the law enforcement area

What is the negotiation of an EU-U.S. data protection 'umbrella agreement' for law enforcement purposes about? What's the objective?

The EU and the U.S. are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement") (IP/10/1661). The EU's objective in these negotiations is to ensure a high level of data protection, in line with the EU data protection acquis, for citizens whose data is transferred across the Atlantic, thereby further strengthening EU-U.S. cooperation in the fights against crime and terrorism.

The conclusion of such an agreement, providing for a high level of protection of personal data, would represent a major contribution to strengthening trust across the Atlantic. Following the EU-U.S. Justice and Home Affairs Ministerial on 18 November, the EU and U.S. committed to "complete the negotiations on the agreement ahead of summer 2014".

What are the demands of the EU in the negotiation?

The high level of protection provided for personal data should be reflected in agreed rules and safeguards on a number of issues:

- Giving EU citizens who are not resident in the U.S. enforceable rights, notably the right to judicial redress. Today, under U.S. law, Europeans who are not resident in the U.S. do not benefit from the safeguards of the 1974 US Privacy Act which limits judicial redress to U.S. citizens and legal permanent residents.

At the EU-U.S. justice and home affairs ministerial a commitment was made to address this issue: *"We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014."*

- Purpose limitation: How and for what purposes the data can be transferred and processed;
- Conditions for and duration of the retention of the data;
- Making sure that derogation based on national security are narrowly defined

An "umbrella agreement" agreed along those lines, should provide the general framework needed to ensure a high level of protection of personal data when transferred to the U.S. for the purpose of preventing or combating crime and terrorism. **The agreement would not provide the legal basis for any specific transfers of personal data** between the EU and the U.S. A specific legal basis for such data transfers would always be required, such as a data transfer agreement or a national law in an EU Member State.

4. Using the existing Mutual Legal Assistance agreement to obtain data

What is the Mutual Legal Assistance agreement (MLA)?

Mutual legal assistance agreements consist of cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance to obtain evidence located in another country. This also entails requests by law enforcement authorities to assist each other in cross-border criminal investigations or proceedings. Mechanisms have been put in place both in the EU and in the U.S. to provide a framework for these exchanges.

The EU-U.S. Mutual Legal Assistance agreement is in place since 2010. It facilitates and speeds up assistance in criminal matters between the EU and the U.S., including through the exchange of personal information.

If U.S. authorities circumvent the Mutual Legal Assistance agreement and access data directly (through companies) for criminal investigations, they expose companies operating on both sides of the Atlantic to significant legal risks. These companies are likely to find themselves in breach of either EU or U.S. law when confronted with such requests: with U.S. law (such as for example, the Patriot Act) if they do not give access to data and with EU law if they give access to data. A solution would be for the U.S. law enforcement authorities to use formal channels, such as the MLA, when they request access to personal data located in the EU and held by private companies.

Negotiations on the Umbrella Agreement provide an opportunity to agree on commitments that clarify that personal data held by private entities will not be accessed by law enforcement agencies outside of formal channels of co-operation, such as the MLA, except in clearly defined, exceptional and judicially reviewable situations.

What is the U.S. Patriot Act?

The U.S. Patriot Act of 2001 is an Act of Congress that was signed into law by U.S. President George W. Bush on October 26, 2001. It permits the Federal Bureau of Investigation (FBI) to make an application for a court order requiring a business or another entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a U.S. citizens or to protect the country against international terrorism or clandestine intelligence activities. The order is secret and may not be disclosed.

In the course of the EU-U.S. Working Group's meetings, the U.S. confirmed that this Act can serve as the basis for intelligence collection which can include, depending on the programme, telephony metadata (for instance, telephone numbers dialled as well as the date, time and duration of calls) or communications content.

5. Addressing European concerns in the on-going U.S. reform process

How will the U.S. review of U.S. surveillance programmes benefit EU citizens?

U.S. President Obama has announced a review of U.S. national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised following recent revelations about U.S. intelligence collection programmes. The most important changes would be **extending the safeguards available to U.S. citizens and residents to EU citizens not resident in the U.S., increased transparency** of intelligence activities, and further **strengthening oversight**.

More transparency is needed on the legal framework of U.S. intelligence collection programmes and its interpretation by U.S. Courts as well as on the quantitative dimension of U.S. intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of U.S. intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

Such changes would restore trust in EU-U.S. data exchanges and in the digital economy.

What about federal U.S. legislation on Privacy?

In March last year, immediately after the Commission's reform proposals were adopted, the White House announced that it would work with Congress to produce a "Consumer Privacy Bill of Rights".

The recent discussions in Congress testify to the growing importance attached to privacy in the U.S. as well. An IPSOS poll released in January 2013 says that 45% of U.S. adults feel they have little or no control over their personal data online. In addition, there is also no single U.S. Federal law on data protection. Instead, there is a maze of State laws offering varying degrees of security and certainty. In Florida, not a single law lays down a definition of "personal information". In Arizona there are five. The same goes for rules on security breaches. Some States have them, others do not.

Once a single and coherent set of data protection rules is in place in Europe, we will expect the same from the U.S. This is a necessity to create a stable basis for personal data flows between the EU and the U.S. Inter-operability and a system of self-regulation is not enough. The existence of a set of strong and enforceable data protection rules in both the EU and the U.S. would constitute a solid basis for cross-border data flows.

6. Promoting privacy standards internationally

What can be done at global level?

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the U.S. A high level of protection of personal data should also be guaranteed for any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

The U.S. should accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), as it acceded to the 2001 Convention on Cybercrime.

Will Data Protection standards be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership?

No. Standards of data protection will not be part of the on-going negotiations for a Transatlantic Trade and Investment Partnership. The European Commission makes this very clear in today's Communication.

This has been confirmed by Vice-President Reding and Commissioner de Gucht on several occasions. As Vice-President Reding stated in a recent speech: "*Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable.*" ([SPEECH/13/867](#))

7. EU-U.S. Working Group on Data Protection

When was the EU-U.S. Working Group on Data Protection established?

The ad hoc EU-U.S. Working Group on data protection was established in July 2013 to examine issues arising from revelations of a number of U.S. surveillance programmes involving the large-scale collection and processing of personal data. The purpose was to establish the facts around U.S. surveillance programmes and their impact on personal data of EU citizens.

The Council of the European Union also decided to establish a "second track" under which Member States may discuss with the U.S. authorities, in a bilateral format, matters related to national security, and questions related to the alleged surveillance of EU institutions and diplomatic missions.

How many meetings have been held to date?

Four meetings have taken place. A preparatory meeting took place in Washington, D.C. on 8 July 2013. Meetings of the Group took place on 22 and 23 July 2013 in Brussels, on 19 and 20 September 2013 in Washington, D.C., and on 6 November 2013 in Brussels.

Who participates in the Working Group?

On the EU side, the ad hoc Working Group is co-chaired by the Commission and the Presidency of the Council of the European Union. It is composed of representatives of the Presidency, the Commission services (DG Justice and DG Home Affairs), the European External Action Service, the incoming Presidency, the EU Counter-Terrorism Co-ordinator, the Chair of the Article 29 Working Party (in which national data protection authorities meet), as well as ten experts from Member States, selected from the area of data protection and law enforcement/security. On the U.S. side, the group is composed of senior officials from the Department of Justice, the Office of the Director of National Intelligence, the State Department and the Department of Homeland Security.

What have been the main findings of the Working Group?

The main findings of the Working Group have been the following:

- A number of U.S. laws **allow the large-scale collection and processing of personal data** that has been transferred to the U.S. or is processed by U.S. companies, **for foreign intelligence purposes**. The U.S. has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in U.S. law laying down specific conditions and safeguards.
- **There are differences in the safeguards applicable to EU citizens compared to U.S. citizens whose data is processed**. There is a lower level of safeguards which apply to EU citizens, as well as a lower threshold for the collection of their personal data. In addition, whereas there are procedures regarding the targeting and minimisation of data collection for U.S. citizens, these procedures do not apply to EU citizens, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. While U.S. citizens benefit from constitutional protections (respectively, First and Fourth Amendments) these do not apply to EU citizens not residing in the U.S.
- **A lack of clarity remains as to the use of some available U.S. legal bases authorising data collection** (such as some 'Executive Order 12333'), the existence of other surveillance programmes, as well as limitations applicable to these programmes.
- Since the orders of the Foreign Intelligence Surveillance Court are secret and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues (judicial or administrative), for either EU or U.S. data subjects to be informed of whether their personal data is being collected or further processed. **There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.**

- While there is a degree of oversight by the three branches of Government which applies in specific cases, including judicial oversight for activities that imply a capacity to compel information, **there is no judicial approval for how the data collected is queried**: judges are not asked to approve the 'selectors' and criteria employed to examine the data and mine usable pieces of information. There is also no judicial oversight of the collection of foreign intelligence outside the U.S. which is conducted under the sole competence of the Executive Branch.

For more information:

Press release on the EU-U.S. data flows:

[IP/13/1166](#)